1600.6B
Appendix 1
8/25/78

partment of Transportation

Office of the Secretary

Washington, D.C.

ORDER

DOT 1600.26

11-29-77

AUA TAC
DOCUMENT MANAGEMENT
CENTER

SUBJECT: DEPARTMENT OF TRANSPORTATION PHYSICAL SECURITY MANUAL

1. PURPOSE. The purpose of this Manual is to:

   a. Provide guidance to those directly or indirectly responsible for the development and maintenance of the physical security program at existing or proposed Department of Transportation (DOT) facilities;

   b. Serve as an aid and reference source in the selection and use of security control measures and the avoidance of excessive or unwarranted expenditures for security controls;

   c. Establish basic standards and criteria for the procurement and use of security equipment, and the protection of DOT facilities and property;

   d. Achieve a greater degree of uniformity in the type of protective measures afforded DOT facilities.

2. REFERENCE.

   a. Federal Property Management Regulations, Subpart 101-20.5, Physical Protection, of 6-74, which prescribes policies and methods for the physical protection of buildings and grounds under the charge and control of GSA.

   b. DOT 1600.20, Reporting and Investigation of Violations of Law or Departmental Standards of Conduct, of 1-10-69, which establishes employee responsibilities for reporting and investigating suspected offenses involving violations of law or departmental regulations.

TRIBUTION: All Secretarial Offices
All Operating Elements

OPI: Office of Investigations and Security

c. DOT 1660.2, Theft/Loss Reporting Procedures for the DOT Washington Headquarters Facilities, of 10-3-73, which establishes the procedures for the reporting of all thefts/losses within the DOT Headquarters facilities.

d. DOT 1640.8, Department of Transportation Automatic Data Processing Security, of 11-12-76, which establishes a DOT Handbook for the security of Departmental ADP systems and resources.

e. DOT 1640.4, Classification, Declassification and Control of National Security Information, of 12-12-72, which implements Executive Orders 11652 and 10865.

f. DOT 1600.23, Demonstrations in or Near Government Buildings, of 3-3-72, which promulgates for the Department of Transportation national policy regarding demonstrations at Government buildings.

g. DOT 1620.1A, Use of Weapons by Department of Transportation Personnel, of 8-14-75, which prescribes DOT policy and standards governing the use of weapons by authorized DOT personnel, military and civilian, and by DOT contractor personnel providing law enforcement/security service to DOT facilities.

h. DOT 1660.4, Physical Security Review of New Facilities, Office Space or Operating Areas, of 6-13-75, which prescribes DOT requirements for reviewing the physical security environment when obtaining new facilities, office space or operating areas for use by any DOT element.

i. DOT 1660.1A, Removal of Equipment from Department of Transportation Buildings, of 10-21-74, which establishes controls over the removal of equipment from DOT occupied premises during and after normal duty hours.

FOR THE SECRETARY OF TRANSPORTATION:

R. J. Alfultis
For the Assistant Secretary
for Administration

DEPARTMENT OF TRANSPORTATION PHYSICAL SECURITY MANUAL

TABLE OF CONTENTS

Page

Page

CHAPTER IX

CHAPTER X

CHAPTER XI

CHAPTER XII

ATTACHMENTS

ATTACHMENT 1 - GSA Federal Protective Service Regional Offices

ATTACHMENT 2 - Bomb Threat Questionnaire

ATTACHMENT 3 - Facility Illumination Standards

ATTACHMENT 4 - Standards for Shipboard Arms and Ammunition Areas

ATTACHMENT 5 - Physical Security Inspection Checklists

ATTACHMENT 6 - Guide to a Facility Protection Plan

CHAPTER I

INTRODUCTION

1-1 PURPOSE. Physical security controls are an essential element in the protection of Departmental facilities and resources. To be effective, such controls must be integrated and complement each other. Using the guidance contained in this Manual, the facility management should, in concert with the servicing security element, take a systems approach in the analysis of the physical protection requirements for the particular facility. It is also important to recognize the limitations of the physical security controls; namely, that they only serve to deter and delay and cannot be expected to preclude a determined intruder from penetrating a facility for illicit purposes.

1-2 SCOPE. This Manual is limited in scope to the salient aspects of physical security, covering such varied topics as access controls, physical barriers, guards, security cabinets, destruction equipment, contingency plans, inspection procedures, etc. Because of the broad range and disimilarity of facilities within DOT, the guidance set forth in the individual chapters must be tailored to fit the particular needs of each facility, recognizing that every facility, regardless of its size or physical composition, has a need for some degree of security control.

1-3 DEFINITIONS. For purposes of this Manual, the following definitions apply:

a. Facility is any manned or unmanned structure or space owned by DOT or leased by or for DOT, regardless of its size, configuration or location.

b. Physical security is that part of an overall security program which is intended to apply physical measures for the protection of personnel, facilities, materials, equipment, and documents against threats, other than overt military action.

c. Servicing Security Element is that DOT organizational element which provides security services for DOT facilities within its assigned jurisdiction, irrespective of whether or not the security element is physically located at the particular facility.

1-4 GENERAL. Physical security controls are designed primarily to preclude and/or minimize the effects of both natural and man-made hazards. While some facilities may be more vulnerable to different types of hazards than others, such factors must be considered when conducting a risk analysis of each facility.

a. Natural Hazards. Natural hazards are usually the consequence of natural phenomena, although some can be induced by human actions. Although natural hazards normally cannot be prevented by physical security measures, it is essential to remember that natural hazards

will greatly affect security operations. Protective measures must be increased when natural hazards exist. Natural hazards may also reduce the effectiveness of security measures already in effect. Due to the effects of these natural hazards, perimeter fences may be down, protective lights and alarms systems may not operate, patrol vehicles may be damaged, and property may be scattered over a large area. Any one or a combination of these effects will require immediate reinforcement of the security force and implementation of additional physical protection measures. Physical security plans must be closely coordinated with facility emergency and disaster plans. Effects of some natural hazards are:

(1) Floods - flooding of the facility with resulting property damage, destruction of perimeter barriers, and short circuiting of alarm devices. Heavy rains, or snowfalls, even though they do not result in floods, may cause some of the same damage.

(2) Storms - high winds or rain causing alarm devices to short circuit, creating nuisance alarms and limiting visibility.

(3) Earthquakes - causing nuisance alarms, possible fires from broken gas mains, buildings weakening and collapsing.

(4) Winds - disrupting power lines, setting off nuisance alarms, causing hazards with flying debris.

(5) Snow and ice - blocking roads, delaying response time to alarms, and the freezing of locks and alarm mechanisms.

(6) Fires - damage/destruction of natural and physical perimeter barriers and buildings.

b. Man-Made Hazards. They include acts of commission or omission both covert and overt, which could disrupt or destroy the operation or mission of the facility. Security planning must be based on the assumption that a risk does exist from such hazards. Examples are the following:

(1) Industrial accidents - explosions and fires.

(2) Civil disturbances - riots and other acts of civil disobedience that may threaten the security of the facility.

(3) Bomb threats.

(4) Hostage situations.

(5) Sabotage - incendiarism, explosives, and mechanical or contamination sabotage.

(6) Pilferage.

(7) Carelessness and accidents which could disrupt operations, destroy critical material, and inflict casualties among key personnel.

1-5 PROPOSED CHANGES. Users of this Manual are encouraged to submit, through appropriate channels, recommended changes and comments to improve this publication. Comments should be keyed to the specific chapter, page and paragraph in which the changes are recommended. Justification for the proposed change should also be provided in order that it may be properly evaluated. As changes occur in the state-of-the-art which may affect the contents of this Manual, they will be published on an "as needed" basis.

CHAPTER II

2-1 SECURITY PLANNING. Once a decision is made to select, construct, reconfigure a facility or move into another facility, security considerations should be an integral part of the planning. The servicing security element should participate in the site-selection process and become involved in the initial design stages. The failure to introduce security factors into the planning and design stages can often prove to be a costly or uncorrectable mistake. In determining the level of security required for a particular facility, the security element should be guided by the general criteria for categorizing DOT facilities set forth in Chapter XI.

2-2 SUPERVISION OF DESIGN. The earlier the architect is made aware of the security requirements the better it is for all concerned. He is not a "security man" and must look to the security staff to guide him through the design stages. Any change made after the preliminary site design has been completed by the architect will be expensive. While an optimum level of protection at a facility is the desirable objective, it is not always attainable due to fund limitations and other factors. It is also essential that the security personnel maintain a dialogue with the architects in order to insure that the basic security controls remain in the design.

2-3 DESIGN FACTORS. Key factors that should be considered in security planning are:

a. Personnel Entrances. There are two prime reasons for controlling entrances -- to control access and prevent thefts. The more entrances there are the more difficult and expensive the controls become. A basic objective should, therefore, be to have a minimal number of entrances to the facility. To reduce the number of entrances in a facility which is comprised of a number of separate buildings, such buildings should be grouped as close together as possible. An interconnecting barrier could then be designed which would permit the facility to be treated as one building for control purposes. Another way of limiting the entrances is to locate the parking lot in one area on the site, thereby creating the need for only one pedestrian gate or door for entering the facility. Having one entrance, for example, with a number of aisles to handle personnel traffic is also preferred to having four entrances on four sides of a facility. When there are multiple entrances, it may be possible to close one or more of them during slack periods.

b. Safety and Fire Protection. The emergency exits needed to satisfy safety and local building code requirements may be met by equipping them with panic hardware. Alarms can be installed on such exits, which will annunciate when they have been opened. Because of the close interrelationship between security, safety and fire protection, they should be considered collectively in the planning of the facility. Particular attention should be given to need for, and location of, sprinkler systems, smoke detectors, pumps, hoses, hydrants, etc.

c. Utilities. Utility systems vital to the continued operation of the facility located within the interior of the facility should be protected against tampering, vandalism and sabotage. Such utilities would include, but not be limited to:

(1) Telephone and electrical closets;

(2) Power generators (including emergency power supply);

(3) Main control valves and regulators;

(4) Water supply;

(5) Boilers;

(6) Air conditioning rooms; and

(7) Transformers.

d. Organizational Layout. In the facility planning stages, special emphasis should be placed on the internal configuration of the facility and the proper placement of the organizational elements having security considerations. The location of a function can often serve as an effective safeguard and deterrent against unauthorized entry or theft. For example, locating the imprest fund in a segregated area that is as far removed as possible from the stairwells and elevators will reduce the likelihood of a robbery.

(1) Typical of the activities that deserve special consideration in the layout of a facility are:

(a) Imprest funds, including sub-cashiers;

(b) ADP activities;

(c) Communications Centers;

(d) Medical facilities;

(e) Equipment storage rooms;

(f) Weapons storage areas;

(g) Shipping and Receiving areas;

(h) Classified work areas;

(i) Mailrooms;

(j) Utility rooms; and

(k) Warehouse areas.

(2) Once these activities are identified, security personnel should insure that the necessary construction features are provided for in the facility design and also monitor the actual construction of the facility. Security personnel should insure that any alteration in the facility design is coordinated with them.

2-4 REDESIGNING EXISTING FACILITIES. Security planning for facilities that are to be reconfigured is as important as that for new facilities. The security costs that may be incurred through changes in the configuration of the facility (or internal movement of functions) can increase sharply if the security factors are not weighed carefully beforehand. On the other hand, the redesign of a facility for the purpose of increased protection might prove to be economically sound when the cost is compared with the corresponding reduction in the theft rate and manpower that could be achieved.

2-5 COMMERCIALLY-LEASED OFFICE SPACE. There are a number of DOT activities occupying space in commercially-owned buildings. The common arrangement is for GSA to execute the lease on behalf of the Government. Usually, there will be non-DOT tenants in the buildings, consisting of both Government and commercial occupants. From a security standpoint, this creates several problems. First, access to the DOT space, particularly after normal duty-hours, cannot realistically be controlled to the same degree as in a facility where DOT is the sole occupant. Second, the DOT tenants must often rely on GSA to establish the basic protection plan for the building who, in turn, must work through the building owner whenever any structural changes are to be made. Finally, there is often the problem of having to obtain security support or assistance from the servicing DOT security element which may be located a considerable

distance from the building. (Attachment 1 lists the addresses and phone numbers of the GSA Federal Protective Services Regional Offices.) It is of prime consideration that every effort be made to implement the basic physical control measures prior to, rather than after, occupancy. This has the dual advantage of, first, giving assurances that the DOT space and property will be afforded protection from the time of initial occupancy; and, second, of avoiding the cost of redesigning the space for security reasons at a later date. Some of the factors that are highlighted in DOT 1660.4 are:

a. Selecting Space.

(1) Avoid, if possible, separating or scattering offices throughout the building.

(2) Attempt to locate the offices on the top rather than the lower floors.

(3) If there is a mixture of DOT elements in the same building, make an effort to locate them on the same or successive floors.

b. Controlling Access into the Space.

(1) Equip with a locking system which gives the tenant effective control over who can get into the space during security hours when the space is normally unattended.

(a) Provide for perimeter doors to be locked and for the locking of interior rooms if needed.

(b) Assure effective key controls and lock changes if keys become compromised.

(2) If admittance is screened by a guard force, specify how authorized persons are to be identified.

(3) Unless cleaning and building maintenance/repair is performed during normal duty hours, determine how their presence during security hours is controlled.

(4) If elevator service is provided for the space, assure that it does not give uncontrolled access during security hours.

c. Controlling Removal of Property, Equipment and Official Records.

(1) Specify what property removal controls are applicable and report all property thefts (see DOT 1660.1A).

(2) Provide added protection for windows which are easily accessible from the exterior and are not under guard observation.

(3) Place activities requiring most protection (e.g., involving funds, sensitive information, etc.) in strategic locations in space with minimum vulnerability.

(4) Determine how covert exit can be prevented without infringing on safety requirements.

d. Obtaining Protective Services.

(1) Utilize available protective forces provided by GSA, the building owner or the tenant agency.

(2) When no immediate guard service is available, establish liaison with local law enforcement officials, advising of the security hours and whom to contact in an emergency.

(3) Arrange for employee parking facility protection if needed.

2-6 CONTINGENCY PLANS. Contingency plans must be developed for all DOT manned facilities. Also, in accordance with 41 CFR 101-20.504.2, all agencies which occupy buildings and grounds for which GSA has space assignment responsibility are required to develop and implement a facility protection plan to safeguard life and property in the event of all emergencies, except for enemy attacks. The term "emergency" includes situations occasioned by bomb threats, civil disorders, fires, explosions and natural disasters. Within DOT, the term also embraces threats directed specifically at ADP facilities and classified material. Described below are the guidelines that should be followed in the development of the protection plan. (Additional guidance is contained in Attachment 6.)

a. Preparation of the Plan. The responsibility for the development and coordination of the protection plan is normally that of the servicing security element. However, the responsibility for developing all or a portion of the plan may be delegated to the management of the facility, provided that the plan is submitted to, and approved by, the security element. Necessary coordination should be effected with other elements having an assigned role in the execution of the plan. Designated employees who are a part of the organizational staff should be specified in writing and trained in carrying out their assigned functions.

(1) In facilities where DOT is not the sole tenant (e.g., a Federal Office building having multiple Government tenants) the agency

having the largest number of employees has, in accordance with the provisions of 41 CFR 101-20.504-2, the primary responsibility for developing the facility's protection plan and for coordinating the plan with the other tenants. The only exception to this criteria would be if an agreement is reached among all of the agencies in the facility to designate another agency, other than the largest one, to prepare and coordinate the plan. In some instances it may be necessary for DOT tenants to exercise the initiative in developing the protection plan independent of, or in concert with, the other agencies in the building.

(2) In leased space, GSA will coordinate activities with the primary occupant agency and the lessor to insure that a comprehensive plan is available for the occupants of the GSA-leased space. The GSA representative (building manager) is required to assist the occupant agency(ies) and cooperate with the local authorities in achieving the objectives of the Plan. Such assistance will normally consist of providing the occupants with publications dealing with emergencies in Federal buildings and technical help in, for example, the operation of the utility systems and the installation and maintenance of warning devices and firefighting apparatus.

b. Activation of the Plan. As indicated in 41 CFR 101-20.504-2, the decision to activate the protection organization is a critical one, based on such factors as the up-to-the-minute intelligence, tensions in the locality, previous experience, sensitivity of the facility and the advice of the local, state and Federal law enforcement agencies. Of course, when there is an immediate danger to persons because of an actual fire, or explosion or the discovery of an explosive device, then the premises must be evacuated by sounding the fire alarm or other means prescribed in the Plan. The decision to evacuate or not to evacuate a facility rests with the official designated with such authority in the protection plan based on the advice and counsel of the servicing security element. To evacuate a facility prematurely or without ample cause, as in the case of a bomb threat, is not only disruptive to the operation but also lends encouragement to the person making the threat. Activating the emergency plan after normal duty hours does not, of course, pose the same problems as it would when the facility is fully occupied, if for no other reason than there are less people in the building and less likelihood of disrupting the operation. In either case, however, the designated official must exercise the same prudent judgment in deciding whether or not to activate the emergency plan. It is also important that the Plan specifically state who is impowered to act for the designated official in his absence, such as during the evening hours or other periods when he may not be readily available.

c. Components of the Plan. The following are some of the more common situations that should be provided for in the Plan, recognizing that no two situations are identical in every detail and that the particular circumstances will dictate the course of action to be taken.

(1) Malicious Damage. Malicious damage is damage or destruction of property when such action results from other than normal use, accidents, or forces of nature, including acts of vandalism, arson, sabotage, etc.

(2) Unauthorized Acquisition of Information. Within DOT, the primary target of any espionage activity would center on the obtaining of classified information or sensitive and proprietary data prior to its public release; such as, economic activity, future allocation of Federal funds, proposed safety standards and regulations and sensitive personnel information. Such information must be identified and afforded a proper degree of physical protection and administrative control during periods of emergency.

(3) Bomb Threats. While there is no foolproof method of preventing such threats, or preventing their being carried out, the physical security measures and procedures previously discussed will assist in lessening their chances of success. In times of disturbance or on any other indication of dissidence or dissatisfaction, control measures should be intensified. Especially important are personnel identification and control and package and material control. All building occupants,especially security and maintenance personnel should be alert for persons who look or act suspiciously. All personnel should report suspicious objects, items or parcels which do not appear to belong in the area where such items are observed. Doors to utility closets, boiler rooms, fan rooms, telephone wire closets and switchboards, and elevator machinery rooms are especially vulnerable and should be kept locked. Keys must be readily available, however, in the event a search is necessary.

(a) Handling Bomb Threats. Bomb threats may be received either by telephone or by written message. In either case, the immediate question arises as to whether or not the threat is genuine. In some instances, notification of the placement of a bomb has been made by persons who intend only to cause damage to property or equipment and do not want to cause death or injury to personnel. The decision concerning the possible evacuation of the threatened building(s)

or area(s), and the shutting down of utilities, should be based primarily on how valid the bomb threat is considered to be. Another important decision to be made is as to whether or not an announcement of a bomb threat should be made. Such a public announcement may well result in panic. Consideration may be given to making an announcement in a code known only to selected personnel, or disguising it as a practice fire drill. (Note, in a fire situation it is normal to close all doors and windows to delay spread of the fire; in a bomb situation, however, it is better to leave all doors and windows open to dissipate the explosive force.)

(b) Telephone Bomb Threats. Persons likely to receive such a call should be briefed, and trained as necessary, in the following procedures:

(i) Attempt to keep the caller on the line as long as possible to permit tracing and to gather further information.

(ii) Record in writing the exact words of the caller. Attempt to ascertain the location of the bomb, type of device, what it looks like nd expected time of detonation.

(iii) Attempt to determine the sex, the approximate age, and the attitude of the caller, specifically any reasons or motives for his actions in placing the bomb.

(iv) Note any background noise, which may provide a clue to the caller's location.

(v) Note any accent or peculiarity of speech which may help to identify the caller.

(vi) If time permits, ask the caller a question such as "Who is this calling, please, or "What is your name ?"

NOTE: The items listed above may be placed on a locally-devised form, to serve as a checklist and a means of recording information. In appropriate situations, such forms may be distributed to all personnel likely to receive such calls, so that they are familiar with them and are instructed in their use. A sample form, which may be adapted as appropriate, is in Attachment 2.

(4) Civil Disturbances. Civil disturbances are group acts of violence and disorders prejudicial to public law and order and may have an effect on the physical security of a facility. Rioters may breach the perimeter and cause injury to personnel and damage to property of all types through sabotage or looting. Physical security plans must include provisions for the protection of personnel and property in the event of civil disturbances. Such provisions must prescribe specific responsibilities for all actions required to protect personnel and property; they must designate priorities of protection, based on analyses of criticality and vulnerability; and they must be continuously reviewed and revised based on all available intelligence concerning the causes and extent of actual or potential disturbances. (NOTE: DOT 1600.23, Demonstrations in or near Government Buildings, should be consulted for specific guidance on the subject of demonstrations at DOT facilities.)

d. Testing of Contingency Plans. Experience has demonstrated the value of such tests in validating backup provisions; it is not unusual to discover gross deficiencies despite the most careful planning. Similar tests of procedures for fire fighting, loss control, evacuation, bomb threat and other emergencies will give assurance that plans are adequate and workable and will at the same time provide an opportunity for training of personnel. Each test should have a specific objective. A team should be assembled to prepare a scenario for the test, to control and observe the test, and to evaluate the results. This evaluation will provide guidance for modifications to emergency plans and for additional training. The important point is to be sure that the emergency plans have substance and do, in fact, contribute to the security of the facility.

length of the supporting arms and the number of strands can be increased when required. The supporting arms are affixed to the top of the fence posts and are of sufficient height to increase the overall height of the fence at least one foot. Many fences employ a double top guard facing both outward and inward which gives added protection (Figure 3-3). The top guard may be fixed or on springs. The spring type overhang increases the difficulty of scaling the fence. Where a building of less than three stories is used to form a part of the perimeter, a top guard should be used along the outside coping to prevent access to the roof.

3-6 DESIGN OF PHYSICAL BARRIERS. The following specifications are set forth as guidelines for planning and designing physical barriers.

a. Fences: Fences should be extended to within 2 inches of firm ground. They should be located not less than 50 feet nor more than 150 feet from the location of interior buildings or object of protection. They should be designed so there is at least 20 feet clearance between perimeter barriers and exterior structures, parking areas, or other natural features which would offer concealment or facilitate unauthorized access to the protected area. Where this is not possible due to property lines, the location of a facility, or adjacent structures, the perimeter barriers should be increased in height.

b. Other barriers. Where walls, roofs, doors or windows, or combinations thereof serve as barriers, they should, in general, be of such construction and be so arranged as to provide protection equivalent to that provided by chain link fencing. For example, when masonry walls provide the perimeter barrier, they should be of minimum height specified for fencing and augmented by the barbed wire topping. When of less than the specified minimum height, they should be topped with chain link fencing (or equivalent) to attain the minimum height requirements. Under some circumstances it may be desirable to increase the height of the fence gradually until it is double the original height at the point where it meets the building. When a building constitutes part of the perimeter barrier, it is not necessary to supplement it with fencing, provided that the side of the building facing the perimeter does not offer any potential points of ready access.

3-7 PERIMETER ENTRANCES.

a. The number of gates and perimeter entrances in active use should be limited to the minimum required. This is mainly a matter of having sufficient entrances to accommodate the peak flow of both pedestrian and vehicular traffic, and adequate lighting for rapid and efficient

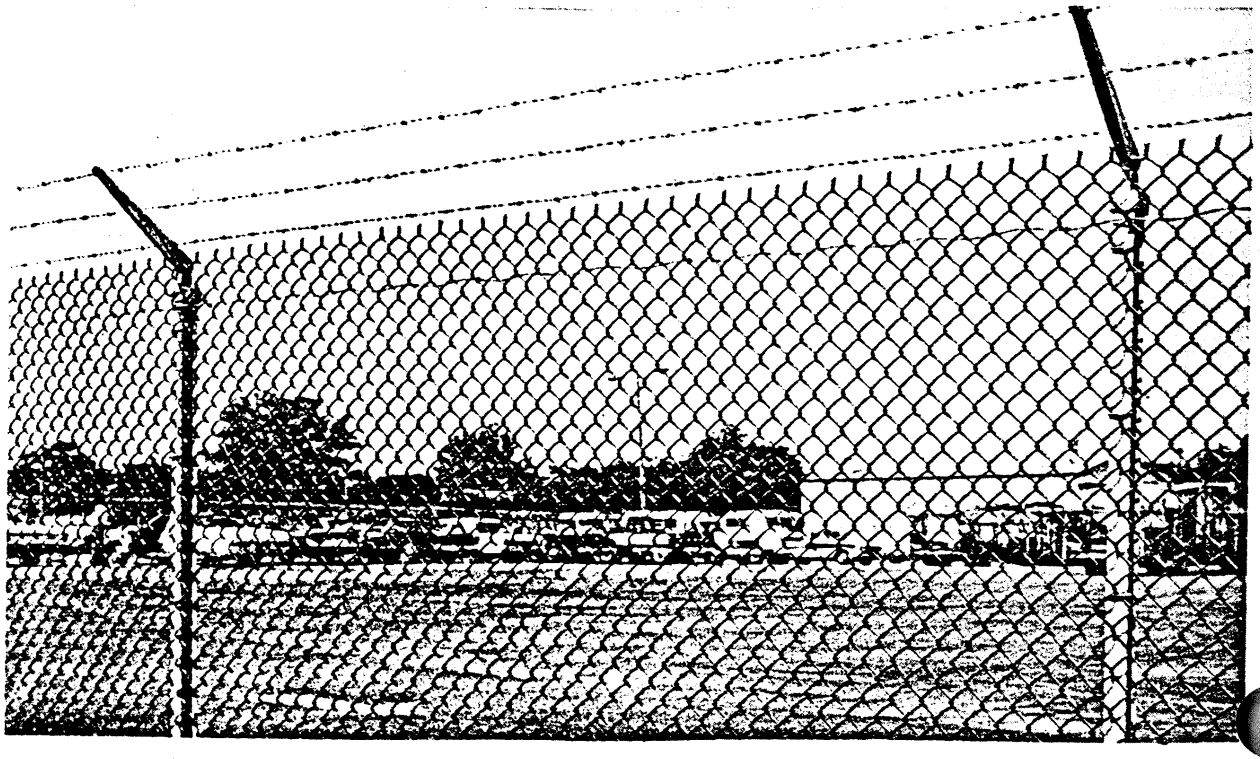


FIGURE 3.2 - CHAIN LINK FENCE WITH TOP GUARD

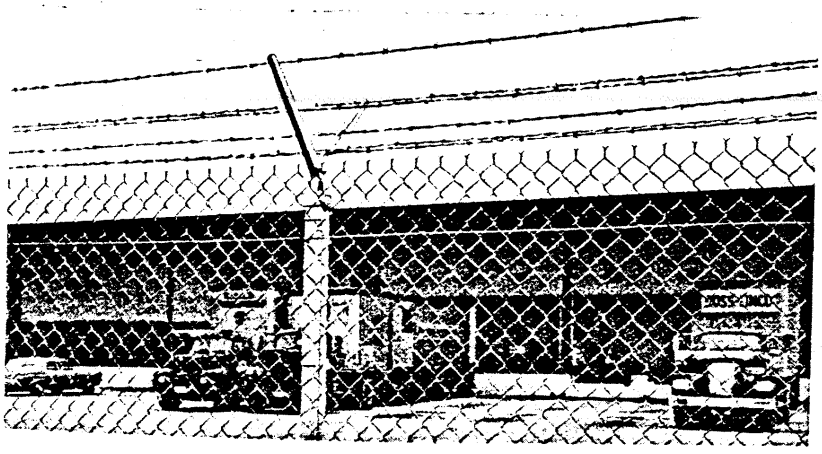


FIGURE 3.3 - DOUBLE TOP GUARD

inspection. When gates are not manned during nonduty hours, they should be securely locked, illuminated during hours of darkness, and periodically inspected by a roving patrol.

b. Semi-active entrances, such as extra gates for use during peak traffic flow, and railroad siding gates, should be locked at all times when not guarded.

c. Inactive entrances (those used only occasionally) should be kept locked and subject to strict key control and inspection.

d. Utility openings which provide access to areas within the perimeter barrier should be locked, guarded, or otherwise provided security equivalent to that of the perimeter barrier.

3-8 PROTECTION IN DEPTH. On a very large installation, such as a large-scale testing facility, it may be impractical to construct an expensive perimeter fence and to keep it under constant observation. Since such an installation is usually established in a sparsely inhabited area, its comparative isolation provides reasonable perimeter protection. Under these circumstances the posting of warning signs or notices, the reduction of access roads, and periodic patrols in the area between the outer perimeter and the inner area of the installation may be sufficient.

PROTECTIVE LIGHTING.

a. This safeguard has considerable value as a deterrent to thieves and vandals. It is an essential element of an integrated physical security program.

b. Requirements for protective lighting at facilities will depend upon the situation and areas to be protected. Each situation requires careful study to provide the best visibility that is practicable for such security functions as checking of badges and people at entrances, inspection of vehicles, prevention of illegal entry, detection of intruders both outside and inside buildings and other structures, and investigation of unusual or suspicious circumstances. Where such lighting provisions are impractical, additional security posts, patrols, or other security means will be necessary.

c. When planning protective lighting the following should be considered:

(1) Adequate illumination to discourage or detect attempts to penetrate an area and to reveal the presence of unauthorized persons within the area.

(2) Light sources located to insure that illumination is directed toward probable courses of intruders.

(3) Shadowed areas caused by structures near or adjacent to vital areas should be illuminated.

(4) Design should provide for overlapping light distribution, and protection against intentional damage.

(5) Emergency power should be included for the protective lighting. Controls and switches should be locked at all times. A central station for locating these devices should be provided. (See Attachment 3 for specific illumination standards.)

3-10 PERIMETER INTRUSION DETECTION. The primary means of perimeter protection continues to be personal observation. However, such observation is usually limited to that performed by periodic patrols. Intrusion detection devices may be a valuable additional security aid if the perimeter requires continuous surveillance. The decision to use such devices depends upon the vulnerability and sensitivity of the protected area, the degree of protection deemed necessary, and the security aids currently in use. Chapter VIII provides guidance on many types of intrusion detection systems and equipment which may be used for perimeter security.

3-11 DEVICES FOR GATE PROTECTION.

a. Usually, gates are protected by the use of locks and intermittent patrol checks, or by fixed posts. Intrusion detection devices at gates are not normally justified. However, if the gate is used only intermittently, or if additional protection is desired for the gate portion of the perimeter fence line, some such device may be usefully employed. Among the various devices that may be employed for controlling access at the gates are coded card keys, pushbutton combination and closed-circuit television (CCTV). Described below are some factors to be considered in the use of CCTV.

b. CCTV, while not an alarm device in itself, is very useful in physical security operations and is frequently used as an admittance control or to complement an alarm system. This may be accomplished by placing cameras at critical locations with direct visual monitoring from a remote vantage point (Figure 3-4).

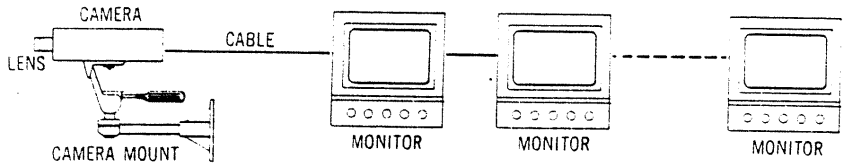
c. Closed circuit television may be used on gates that are not manned continuously. This system normally consists of a television camera,

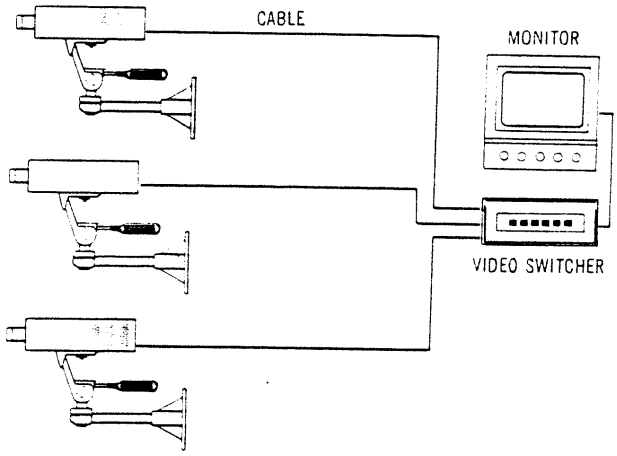
monitor, and electrical circuitry. The camera may be remotely controlled by the monitoring personnel. TV on gates may include the use of a two-way communication system between the monitor panel and the gate lock. With this device, the person at the monitor panel can be alerted on the speaker by a person desiring to enter, determine his authority to enter and then release the gate lock.

d. TV controls should be enclosed in metal housing and properly secured to preclude any tampering by unauthorized personnel.

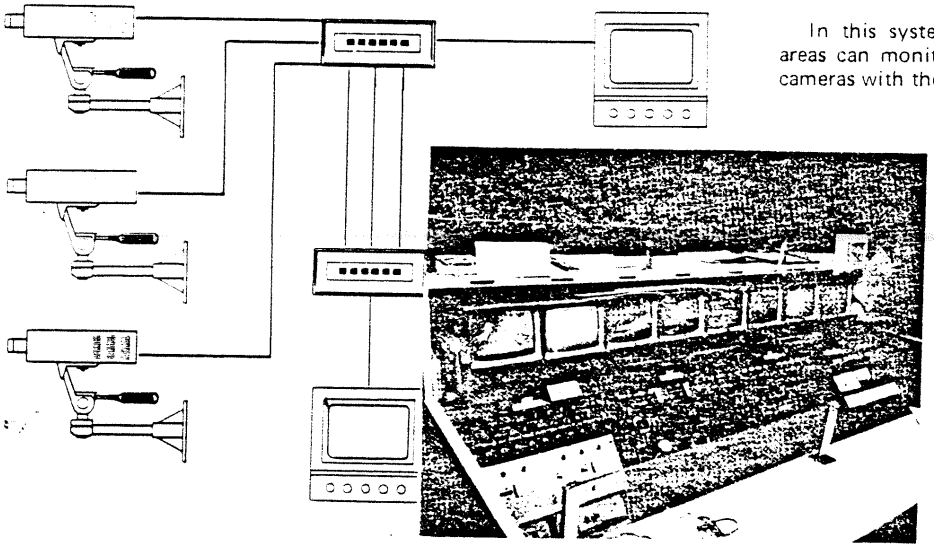
e. One problem in TV usage is the light intensity required for some cameras. This requirement must be considered before the system is purchased and installed. TV cameras are available which operate on a low light level. Their cost, however, is greater than others which require higher light levels. Other factors which must be considered are the initial cost of the system and weather conditions.

A simple system to cover a limited area may just require one camera and three monitors as shown at left.





Or, to reverse the requirements, where the areas need to be covered with only one guard on duty, you can have three cameras and one monitor and a switcher.



In this system, viewers in two different areas can monitor areas surveilled by three cameras with the aid of two switchers.

FIGURE 3-4. CCTV "AREA" SYSTEM

CHAPTER IV

4-1 BUILDING CONTROLS. After an adequate perimeter defense has been designed, or if the buildings themselves constitute the perimeter barrier, the next line of defense at the exterior of the buildings must be planned (Figure 4-1). The extent to which the building exterior has to be secured is dependent on a number of variances; for example, the relative criticality of the facility, its location, whether it is manned or unmanned and working hours. Consideration should be given to securing any opening 96 sq. in. or larger and which is less than 18 feet above the ground. The roof, basement, and sides of each building must be examined for potential entrances. The area being protected by this line of defense should be considered to have not only sides but a top and a bottom. The most obvious entrance in this line of defense is through a door or a window. A trespasser may also utilize such openings as manholes, grates that lead to basements, elevator shafts, openings for ventilating equipment, and skylights. The interior area also might be penetrated through the walls or roof of a building.

4-2 DOORS.

a. A door may be an inviting entrance for an intruder because of convenience. Vulnerable points at the door are the frame, the hinges, door panels, and the lock. The door should be installed so that the hinges are located on the inside of the doorway. If this is not possible, the hinges should be installed so that they cannot be removed by taking out the screws or so that they will withstand the use of a chisel or similar cutting device. Also the pins in exterior hinges should not be removable. They should be welded, flanged, or otherwise secured.

b. The door should be of metal or solid wood construction. If a wooden door is not of solid core construction or contains panels less than 1 3/8 inch thick, it can be covered on the inside with at least 16 guage sheet steel attached with screws to provide additional protection.

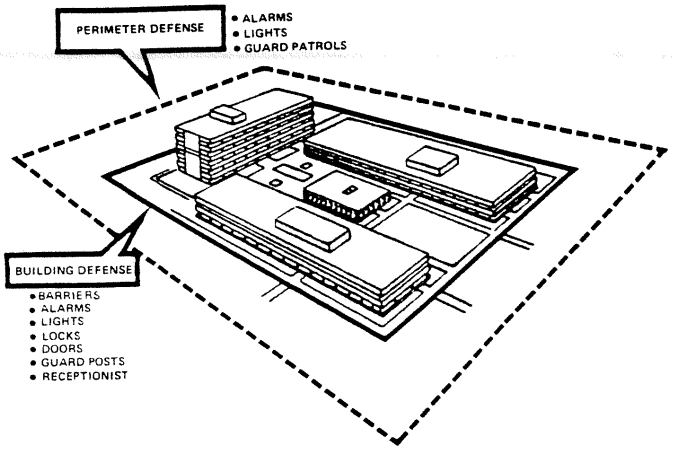


Figure 4.1 – BUILDING DEFENSE

c. Wire mesh (No. 9 guage, 2 inch square mesh) or bars can be used to protect a glass panel in the event it is necessary to utilize this type of door. If iron bars are used, it is generally recommended that the glass panel be covered with bars at least 1/2 inch round or 1 inch by 1/4 inch flat steel material, spaced not more than 5 inches apart. The spacing of the bars would depend upon the type and accessibility of the locking mechanism. Iron or steel grills of at least 1/8 inch material of 2 inch mesh is also considered acceptable protection. If either mesh or bars are used, they should be securely fastened so that they cannot be pried loose. Rounded head flush bolts are usually considered best for this purpose. If possible, mesh or bars should be installed inside the door.

d. Rolling overhead doors not controlled or locked by electric power should be protected by slide bolts on the bottom bar. Chain-operated doors hould be provided with a cast iron keeper and pin for securing the hand chain, while the operating shaft on a crank-operated door should be secured. A solid overhead, swinging, sliding, or accordion garage-type door should be secured with a cylinder lock or a padlock. Also, a metal slide bar, bolt, or crossbar on the inside should be provided. Metal accordion grate or grill-type doors should have a secure metal guide track at the top and bottom and be provided with a cylinder lock or padlock which will provide the necessary protection.

4-3 WINDOWS.

a. Windows are also a possible method of gaining access to a facility. If a window can be opened, it should be secured on the inside. A bolt, a slide bar, or crossbar with a padlock may be used. The window frame must be securely fastened to the building so that it cannot be pried loose and the entire window removed. As with glass panels in a door, it should be remembered that window glass can be broken or cut so that the intruder can reach inside and release the lock. Bars or steel grills may be utilized to protect a window. They should, if possible, be installed in the inside of the window to ensure maximum protection. Iron bars should be at least 1/2 inch round or 1 inch by 1/4 inch flat steel material, spaced not more than 5 inches apart. If a grill is used, the material should be No. 9 guage, 2-inch square mesh. Outside hinges on a window should have nonremovable pins. The hinge pins may be welded, flanged, or otherwise secured so that they cannot be removed.

b. Bars or grills must be securely fastened to the window frame so that they cannot be pried loose.

c. If a window is not needed for ventilation, glass brick will provide maximum security because it is difficult to penetrate. Any part of the window 18 feet or less above the ground can be considered to be a potential easy access point and should be secured.

d. Small panes of glass set in steel framework cannot be considered to be secure construction. An intruder can break a pane of the glass and unlock the window on the inside by reaching his hand through the opening. The metal portion is not intended to give any protection against forced entry. As a result, by breaking several panes of the glass, it is easy to cut or break out the metal framework.

4-4 MISCELLANEOUS OPENINGS.

a. Many sites have manholes which provide entrances into the buildings for service purposes. Others may provide entrances to utility tunnels containing pipes for heat, gas, and water as well as other utilities such as telephone conduit. If a tunnel penetrates into the interior of a building, the manhole cover must be secured to eliminate the potential entrance. A chain and padlock can be used to secure a manhole. Steel grates and doors which are flush with the ground level may provide a convenient access to the basement. These openings may be designed into the facility as service entrances or outside elevator entrances, or they may provide light and fresh air to the basement level. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock. Sewers or storm drains might provide an entrance. If the opening for drains from the facility are sufficient to provide a potential entrance, they should be secured.

b. The roof of a building may erroneously be regarded as secure because it may appear to be difficult to reach. However, an intruder can easily find ways to get onto the roof of a building. It then becomes an excellent point of entry because a trespasser can often work without being detected. Openings in elevator penthouses, hatchway, or doors to the roof are sometimes overlooked because they may not be used often. These potential access points must be properly secured by locks, bars, etc., and must be inspected periodically to ensure that they have not been left unsecured after use. Skylights are another good source of entry on the roof. These openings can be protected the same way windows are secured -- with bars or mesh. Such protection should, if possible, be installed inside the opening

to make it more difficult to remove. Although a transom may appear to be small, it must not be overlooked as a potential entrance. A simple solution is to seal transoms permanently. However, if it is decided that they are needed, each transom should be locked from the inside with a sturdy sliding bolt lock or other similar device or be equipped with bars or grills.

c. Ventilating shafts, vents, or ducts, along with openings in the building to accommodate ventilating fans or the air conditioning system, are also possible entrances. A ventilating shaft or duct may be large enough to provide a potential entry into the building from the outside. A ventilating fan can be removed, or it is sometimes possible to bend the blades enough to make a sufficiently large opening. Screens in a ventilating shaft or duct are generally considered less desirable than bars because screens have a tendency to interfere with the free flow of air.

4-5 FIRE ESCAPES AND BUILDING WALLS.

a. Outside fire escapes will usually not provide an entrance directly into the building. However, if a fire escape is not properly designed, it can provide an easy access to the roof or to openings high above the ground level. Windows or other openings leading off the fire escape should receive special security attention, because a trespasser would find such an opening an easy method of entry if it were not properly secured. The fire escape should not extend all the way to the ground.

b. Walls are normally not considered possible points of entry because of their usual solid construction. However, they cannot be disregarded because intruders break through them to gain entrance. For example, a common wall between two buildings can be a potential hazard. If one of the buildings is of light construction or is not properly secured, the intruder can gain easy access to it. He can then leisurely work his way through the common wall between to reach the area or building to which he wants access. Basement walls may also provide a point of initial entry. Once inside the basement, the intruder can then work to enter the upper part of the building without being so conscious of noise and light.

CHAPTER V

5-1 INTERIOR SECURITY CONTROLS. The third, and perhaps the most important line of defense is the interior controls. (Figure 5-1) If an intruder is able to penetrate the first and second lines of defense (i.e., the perimeter and building exterior controls), the effectivenss of the interior controls takes on added importance. There are also few facilities where every employee would be entitled to have across-the-board access to every area in the facility. Some critical areas, by necessity., have to be "off-limits" if there is to be any semblence of internal security. The extent of the interior controls within the facility will be largely determined by the value and importance of the items and areas to be protected and the vulnerability of the facility to unauthorized entry both during and after normal working hours.

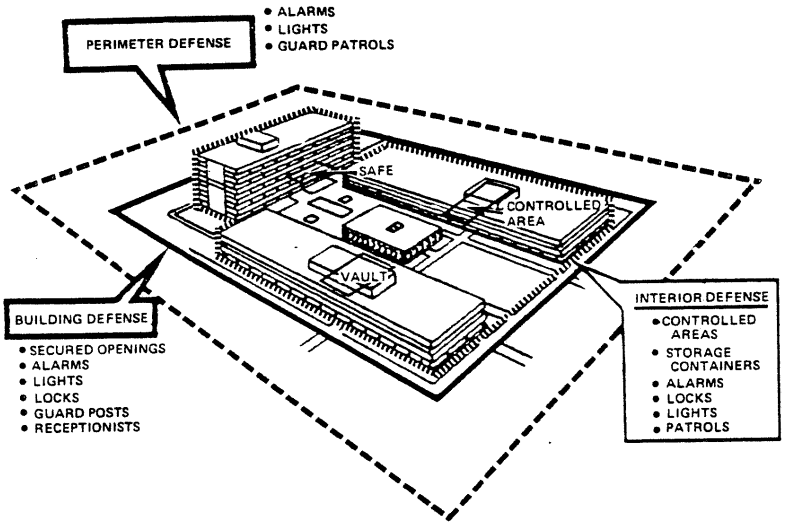


Figure 5.1 – INTERIOR DEFENSE

5-2 CRITERIA FOR THE DESIGNATION OF CRITICAL AREAS. While there can be no fixed criteria for identifying such areas, the following guidelines may be useful in identifying them:

a. Areas necessary for the continuing operation of the activity, which would be difficult to duplicate or restore. Examples: Communication facilities, auxiliary power sources, water supplies, pumps, regulators, telephone and electrical closets, air conditioning rooms, boiler rooms, etc.

b. Areas in which monies or negotiable/sensitive forms are kept, such as:

(1) Government Travel Requests and airline tickets (including ticket stock) in travel offices.

(2) Funds in credit unions and imprest funds.

(3) Purchase order forms (e.g., SF-44's) in procurement or purchasing offices.

(4) Official passports in travel offices.

(5) Credit cards (e.g., AT&T, Government National Credit Card, SE-149) in the issuing offices.

c. Areas which require controlled access in order to preclude interference or disruption of the activities within the area; for example, computer rooms, air traffic control room floors, air traffic control towers, Coast Guard Rescue Control Centers, test facilities, etc.

d. Areas containing classified material which is of such a nature that access to the area is tantamount to having access to the classified information, e.g., classified charts posted on the walls or classified documents stored in open shelves within a vault.

e. Areas used for the storage of valuable or sensitive equipment or data; e.g., loan pools, electronic equipment rooms, warehouse areas, mailrooms, personnel offices, labor relations offices, medical offices, procurement activities, testing areas, etc.

f. Areas which, because of the personnel safety hazards involved, require restricted access.

5-3 CONTROLLING CRITICAL AREAS. Some means of controlling critical areas:

a. Physical segregation from adjacent areas.

b. Employee surveillance of area.

c. Locked rooms (door bell arrangement).

d. Vault-type structure or strongroom.

e. Adequate identification (e.g., coded badges, access lists).

f. Fixed guard post or receptionist stationed at entrance.

g. Electrical/mechanical push-button combination locks.

h. Visitor control (e.g., escorts and sign-in log).

i. Electronic card/key system.

5-4 PROTECTION OF GOVERNMENT FUNDS. The physical security standards outlined below apply to all Government funds which include, without being limited to, revenues and funds of the United States. Funds are primarily considered monies (i.e., coins and currency). However, checks, bonds, etc., should also be considered as falling within this definition. A fund activity is interpreted as any DOT activity or function approved by the head of the DOT facility to handle Government funds; such as, imprest funds, disbursing offices or collection offices. (Although the below requirements do not generally apply to funds controlled by private associations which are physically located within DOT space (e.g., credit unions, employee recreation associations, concessionaires), the servicing security element should encourage such activities to adopt the same or equivalent protective measures in order to decrease the possibility of a robbery or loss of funds.)

a. Responsibilities.

(1) The fund activity custodians have the primary responsibility for insuring that the funds entrusted to their care are protected as prescribed herein, preparing written standard operating procedures (SOP) for safeguarding the funds and insuring that all employees are familiar with the procedures. The SOP should, among other things, outline the action to be taken in the event of a robbery attempt during operating hours and the steps to be taken to reduce the cash on hand to the minimum required for efficient operation.

(2) The servicing security element should (a) coordinate with the fund custodian to insure that adequate protection procedures are developed and implemented; (b) conduct periodic inspections of the security controls to verify that the procedures are being followed and that the physical security controls are functioning properly (e.g., CCTV, "panic" alarms, hold-up cameras, security containers); (c) change, or give instructions in changing, the combination(s) to the containers utilized for the storage of the funds and (d) followup as appropriate on all reports received regarding the loss, shortage or theft of funds.

b. Security Factors. The following factors should be taken into consideration by both the fund custodian and the security element:

(1) The location and type of building in which the fund is situated (e.g., commercially-owned building versus a Government-owned or leased building);

(2) The specific location of the fund (e.g., proximity to elevators and stairwells, and whether or not it is located in a segregated area as opposed to an open work area);

(3) The relative crime rate in the area which the building is located;

(4) The closeness and response time afforded by the local law enforcement authority.

c. Administrative Safeguards. Fund activities require various procedural safeguards to protect the funds and the employees concerned, including, but not limited to, the following:

(1) Screen from public view as much of the handling of funds as practicable.

(2) Develop emergency procedures to follow in event of a hold-up or other critical situations.

(3) Obtain advances in the form of several checks, to be cashed only as needed.

(4) Perform sizeable cash transfers in an inconspicuous and non-routine manner when required.

(5) Provide an escort (armed or unarmed depending on local conditions) to move funds in excess of $2,000 between the fund activity and depositories.

(6) Maintain accountability protection for alternates and subcashiers by providing separate cash boxes or safe drawers.

(7) Avoid the intermingling of funds with classified material and items of intrinsic value.

(8) Require positive safe closing and checking procedures when the fund is unattended during the work day and at close of business.

(9) Limit to a minimum the employees allowed access to the storage container and the lock combination and changing the combination as required. (See subparagraph e(2) below.)

d. Fund Storage.

(1) For funds averaging $500 or less on hand:

(a) Funds shall be stored, preferably, in a GSA-approved security container which has an internally fixed label stating the Federal Specification it was manufactured under and the security protection it affords and an external label reading: "GENERAL SERVICES ADMINISTRATION APPROVED SECURITY CONTAINER (MANUFACTURER'S NAME)"; or,

(b) In a metal file cabinet equipped with a steel bar and secured by a three position, dial-type, changeable combination padlock (see Chapter X, paragraph 10-9b. for approved padlocks).

(2) For funds averaging more than $500 but less than $2,000 on hand:

(a) Funds shall be stored in a GSA-approved security container; and

(b) During non-working hours, entry to the room, building or structure in which the container is located shall be controlled by locked entrances.

(3) For funds averaging more than $2,000 but less than $15,000 on hand:

(a) Funds shall be stored in a Class 1, 2, 4 or 5 GSA-approved security container; or,

(b) In a mercantile safe which meets or exceeds Underwriter Laboratory TL 30 label, or

(c) In any GSA-approved security container provided the specific room in which the container is located, or the container itself, is equipped with an approved alarm system (see Chapter VIII) and the response time to an activated alarm does not exceed 10 minutes.

(4) For funds averaging more than $15,000 but less than $50,000:

(a) Funds shall be stored as prescribed in (3)(a) or (b); and,

(b) The fund storage container shall be located in a fund storage room that meets the criteria set forth in paragraph g. below; and,

(c) The container itself shall be equipped with an approved alarm system.

(5) For funds averaging more than $50,000 on hand:

(a) Funds shall be protected as prescribed in (4) above; and, if practicable,

(b) The funds shall be divided into more than one approved container.

e. Combinations to Storage Containers.

(1) General Precautions:

(a) Lock combination records, including, when applicable, duplicate keys to the cash boxes, shall be given the same degree of protection as the fund. Combination records stored in an alternate repository for emergencies shall be placed in sealed envelopes which are signed and dated across the seal, and which are marked to be opened only in an emergency or when the combination is to be changed.

(b) Combinations shall be memorized by authorized individuals. Records shall not be carried in wallets or concealed on persons or in the office. Knowledge of the combination will be restricted to a minimum number of employees.

(2) Lock combinations shall be changed:

(a) When the container is first put into use.

(b) Annually.

(c) When there is a change of fund custodian or other person authorized to know the combination.

(d) When emergency access to the funds in the absence of the fund custodian is required.

(e) When the combination has been compromised.

f. Supplemental Safeguards. In addition to administrative and storage safeguards, the following supplemental measures should be considered when warranted by the risk factors:

(1) Panic or hold-up alarms.

(2) Closed Circuit Television.

(3) Hold-up camera.

(4) Bullet resistant partitions.

(5) Money clip alarms.

(6) Daytime cleaning.

(7) Single entrance.

(8) Hold-up packets (recorded bills).

g. Fund Storage Rooms. For funds averaging more than $15,000 on hand, the fund storage container shall be located in a storage room as an additional line of defense. Properly designed rooms secured by a proprietary lock can compensate for the absence of a desirable location for the fund activity (e.g., located on the ground floor as opposed to an upper floor). The basic design features that should be included in the construction specifications are:

(1) Walls, Floors and Ceilings. These should be designed to minimize forced or surreptitious entry. Planning should provide for the use of an alarm system to overcome such construction deficiencies as insert-type wall panels and false ceilings, i.e., where the walls do not extend to the true ceilings.

(2) Doors. The number of doors providing access to the room should be kept to a minimum. They should be so constructed as to afford reasonable assurance against forced entry.

(a) Solid doors should be installed or hollow doors covered with 9 to 12 guage security screen or 16 guage sheet steel, fastened with smooth-headed bolts and nuts and peened in place.

(b) Exposed removable hinge pins should be jimmy-proof and, preferably, should be bolted to the inside of the door.

(3) Windows. There will be a minimum number of windows, and all windows will be secured during non-duty hours. If the room has an exterior window or window on a hallway, it will be protected by screens or bars or an intrusion alarm. The frames holding the screens or bars will be securely affixed.

(4) Vents, Crawl Space and Suspended Ceilings. These should be examined to determine whether they would allow illegal entry.

(a) Openings for heating and ventilating ducts will be kept to a minimum. Duct terminals and connection points will be in an exposed location, where they may be readily observed to detect tampering.

(b) Openings of 8 inches or larger will be protected with 9 to 12 guage steel mesh. The steel mesh will either be welded to the duct, or be secured with smooth-headed bolts, with nuts peened in place to prevent removal.

(5) Security Lighting. Night lighting should be provided for any fund container that is visible either from common hallways in the building or from outside the structure.

5-5 PROTECTION OF CONTROLLED SUBSTANCES, DANGEROUS DRUGS AND NARCOTICS. Controlled substances listed in Part 1308 of 21 CFR on Schedules I (opiates), II (opiate derivatives), III and IV (stimulants and depressants), and V (Narcotic drugs) should be stored in a security container listed in the Federal Supply Schedule; or as a minimum, in a safe or filing cabinet having a built-in three position, dial-type combination lock and being of such weight, size, construction or installation as to minimize the possibility of surreptitious entry or forced entry. As an additional safeguard, the container should be placed in a room secured by a proprietary lock and strict accountability maintained over the issuance and control of the keys.

5-6 SMALL ARMS AND AMMUNITION STORAGE AND PROTECTION.

a. Site Selection. Small arms and ammunition shall only be stored in Government facilities. Small arms storage facilities shall not be

located in isolated areas or in any building that is unoccupied for prolonged periods of time. Small arms should, if at all possible, be stored within facilities which are manned 24 hours a day. Criteria for shipboard arms and ammunition storage areas are set forth in Attachment 4.

b. Construction Standards. The following are minimum construction standards for small arms and ammunition storage facilities. (NOTE: If there are only a few weapons involved and they are stored in a GSA-approved security container, then the facility construction standards set forth below are not applicable.)

(1) The room or building shall be constructed of concrete or masonry. The floor and ceiling shall be constructed with material of similar strength.

(2) All doors shall be solid core metal or wood. Wooden doors shall be reinforced externally by 16-guage sheet steel cover, so installed as to preclude easy removal.

(3) Hinge pins shall be concealed or located on the inside of the room. If this is not possible, hinge pins will be spot welded or brazed to prevent removal.

(4) All doors will be secured by a high-security key-actuated padlock (FSN 5340-799-8248) and associated hasp (FSN K2 5340-178-7875).

(5) Windows and other openings shall be bricked-up or shall be protected by 7/8 inch steel pipe or ½ inch steel rod, spaced not more than 4 inches apart, and embedded in concrete or masonry or welded to steel frames securely anchored to the building by smooth head bolts.

(6) Each facility will be protected by an intrusion detector.

c. Protection.

(1) Small arms shall be stored in locked racks (preferably steel) or in Class 5 weapons storage containers. However, if there

is only a very limited quantity of weapons to be protected, they may be stored in any of the other GSA-approved security containers.

(2) Illumination will be provided over all entrances to the arms storage room or building.

(3) If there are windows, lighting shall be maintained within the storage room or building during hours of darkness to facilitate security checks.

(4) All arms and ammunition storage rooms or buildings will be periodically checked by guards.

(5) Where feasible, slides, bolts or other vital parts which render small arms inoperable should be stored separately.

5-7 PROTECTION OF GOVERNMENT PROPERTY. The protection of property, including the prevention of theft of Government supplies and equipment, should be one of the chief concerns of management. Pilferage is probably the most common and annoying hazard and can, if unchecked, assume such proportions as to affect the overall operations of the facility. Pilferage is often difficult to detect, hard to prove and, above all, dangerous to ignore.

a. Theft Factors. Actual losses due to theft depends on a number of factors, among which are:

(1) The type, amount and accessibility of the equipment and supplies and their location within the facility.

(2) The number of persons employed at the facility and the shifts worked, including overtime.

(3) The relative crime rate in the surrounding communities.

(4) The effectiveness of the property management program in terms of conducting physical inventories of accountable property and promptly reporting unexplained shortages or known thefts to the security element, especially for that property referred to as "sensitive" or "personally-attractive" items.

(5) The adequacy of the external and internal physical security controls, plus the use made, for example, of specialized devices for securing in-place office equipment.

(6) The degree to which employees assume personal responsibility for safeguarding property entrusted to their care and their general security consciousness.

b. Theft Targets. Listed below are typical areas in a facility where one would normally expect to find pilferable equipment and supplies. The list is not intended to be all-inclusive, but rather it is designed to serve as a starting point for security elements to use when conducting in-depth security surveys of the facilities under their cognizance. The common denominator in these and similar storage areas is that they usually contain items which lend themselves to concealment, which are of relatively high value and for which markets are readily available.

(1) Shipping and Receiving. Such operations are extremely vulnerable to systematic theft. For instance, it is here that facility employees and truck drivers have direct contact and a readily available means of conveyance which offers a tempting opportunity for collusion. From a physical security standpoint, the shipping and receiving doors should be kept closed when not in use and deliveries, particularly those containing high-value items, should not be left unattended for an extended period of time and certainly not for overnight or weekends. Constructing a secure "holding area" is one means of protecting undelivered high-value items.

(2) Loan Pools. Loan pools are an inviting target because of the wide range of items that usually appear in the inventory (e.g., office equipment, recorders, video and motion picture equipment, cameras, etc.). In addition to segregating and securing the loan pool, the administrative controls must be strictly observed: maintaining current inventory records, establishing a limited charge-out period and following up on overdue items and limiting access to the loan pool. Expendable items such as film and tapes, which are not subject to strict accountability, should nevertheless be afforded adequate physical protection.

(3) General and Specialized Storage Areas. Supplies and equipment which are stored in permanent or semipermanent storage areas or warehouses are vulnerable to theft if adequate precautionary measures are not taken. Access to storage areas containing building materials, automotive and oil supplies, tools, etc., need to be tightly controlled because of the personal use which can be made of such items.

Since they are not ordinarily accounted for in the property management control system, it becomes vitally important that such items be afforded adequate physical protection. In addition, chargeout procedures should be established that would discourage, if not prevent, employees from drawing such materials for other than official purposes. In large warehouses, consideration should also be given to physically segregating high-value items from the general storage area in, for example, wire cages secured by approved combination padlocks. Where storage areas are located in a remote area, they should be given the added protection of an intrusion alarm system. (See Chapter VIII on Intrusion Alarm Systems.)

(4) Miscellaneous Areas. Such special purpose areas as boatyards, hangars, navigational aids, control towers, test vehicles, seaway lock operations, etc., are vulnerable to tampering or interference with their normal operations and should be afforded a reasonable degree of physical protection against unauthorized entry and be posted accordingly.

c. Theft Prevention Measures. The specific measures for prevention of theft will be based on a careful analysis of the conditions at each facility. Some suggested methods for combating losses due to theft are to:

(1) Establish appropriate perimeter fencing, lighting, and parking facilities and effective pedestrian, railway, and vehicle gate security controls.

(2) Establish an effective property removal control system in accordance with the provisions of DOT 1660.1A.

(3) Investigate all thefts/losses quickly and thoroughly.

(4) Maintain an effective key control system.

(5) Maintain adequate security patrols to check buildings, grounds, perimeter, and likely locations which might be used for concealing stolen property.

(6) Install mechanical or electrical intrusion detection devices where practical.

(7) Store bulk quantities of highly pilferable items in enclosed stock areas.

(8) Identify all tools and equipment by some mark or code so that government property can be distinguished from non-government property.

(9) Require charge-out procedures for all tools and equipment.

(10) Insure adequate inventory and control measures are established which account for all material, supplies and equipment.

d. Property Management System. There is a direct correlation between the efficiency of an activity's property management program and the theft prevention program. Each is an indispensable element of the other. If the property accounting and reporting procedures are slipshod or performed in a perfunctory manner, then the likelihood of uncovering stolen or lost property in a timely fashion is significantly decreased. Conversely, if there is a close working relationship between the security and property management offices, the chances of stopping or curbing the thefts increase proportionately. The most common deficiency is the failure (usually inadvertent) on the part of the property custodians and/or the activity's accountable property office to report promptly to the security element any actual or suspected thefts of "in-use personal property" that come to their attention; for example, as a result of the annual physical inventories of personal property. (NOTE: Personal property, as defined in the property management regulations, is all tangible property except real property and records.) It is also not uncommon to find that lost or stolen property has been surveyed and "written-off" by the accounting activity (i.e., removed from the records and accounts) without security having any knowledge of the incident. To prevent this from occurring, the property management procedures should make it clear to the property custodians the importance of reporting any instances of loss, stolen or missing property to the servicing security element, instead of only reporting through the property management channels. The activity's accountable property officer should, in turn, double-check to insure that such reports are being submitted. Some additional points concerning property management are:

(1) The criteria commonly applied for property accountability purposes is that the item must have a useful life of more than one year and a unit value (when acquired) of $300 or more. This figure is usually lowered to $50 for sensitive items which are particularly susceptible to loss or theft; e.g., pocket calculators, adding machines, cameras, recorders, tools and binoculars. Although items of less than $50.00 may not be subject to strict accountability

procedures, they should, nevertheless, be provided adequate physical protection.

(2) Accounting methods are not designed primarily to pinpoint thefts; consequently, such losses may remain undetected or be grouped together with other shrinkages, thus effectively camouflaging them for all practical purposes.

(3) A common assumption is that unaccounted for property is merely misplaced or borrowed and not stolen. This can often prove to be a deceptive and dangerous line of reasoning.

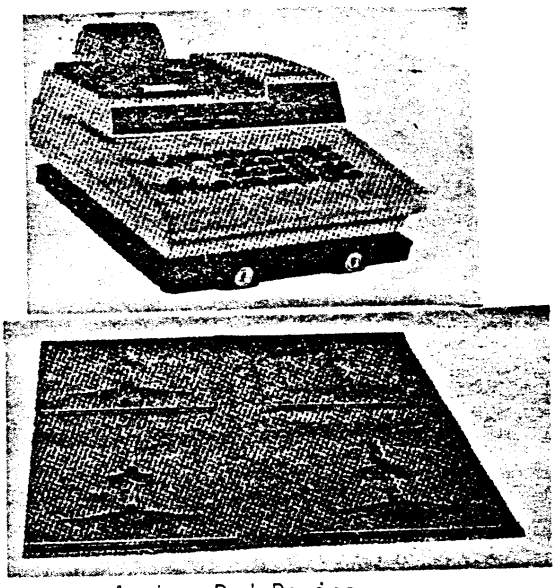
(4) Other factors which can contribute to inventory shrinkages are: the failure to detect shortages in incoming shipments, improper stock usage, poor stock accounting, poor warehousing, improper handling and recording of defective and damaged stock and inaccurate inventories.

(5) In some cases inventory losses may be impossible to detect because of the nature and quantities of materials involved. Stock inventory records may not be locally maintained, or there may be methods for spot checks or running inventories. This is an undesirable situation and should be corrected.

e. Physical Protection of Office Equipment. All office equipment, particularly items valued at $300 or more, such as typewriters, desk calculators, dictating equipment, shall, to the maximum extent possible, be secured in place by a locking device. Exceptions to this requirement may be granted only by the head of the particular facility or activity when it has been determined that special conditions exist that would obviate the need for such security measures. Items of lesser value which do not lend themselves to this approach, such as pocket calculators, cameras, tape recorders, slide projectors, shall be protected at all times when not in use by storing them in locked containers or rooms to which only authorized personnel have access. (Figure 5-2, depicts several of the devices listed on the Federal Supply Schedule.)

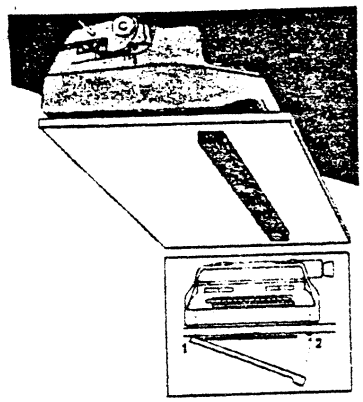
Vertical line denotes change.

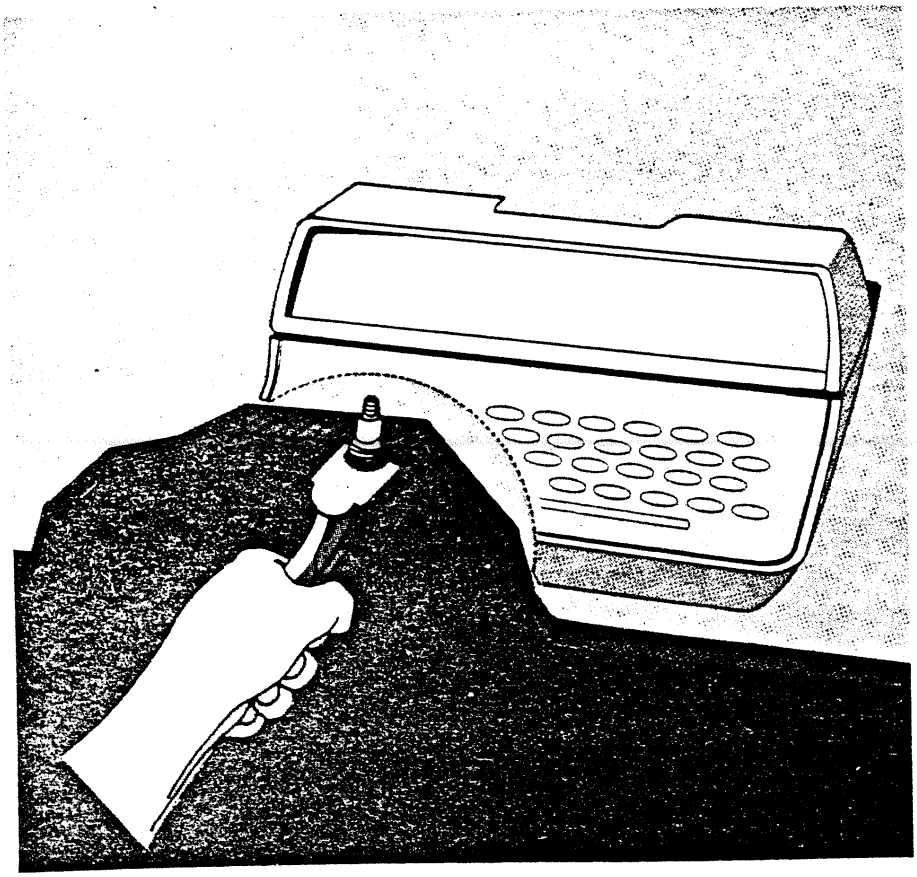
FIGURE 5-2. PROTECTIVE DEVICES



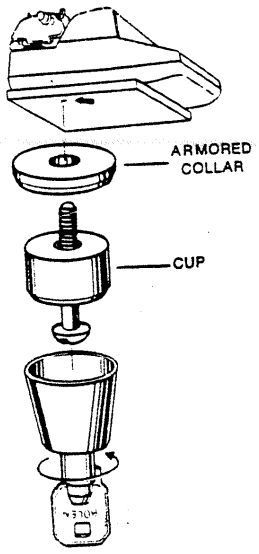
Anchor Pad Device

Two Point
Locking Device





Desk Top
Locking Device



CHAPTER VI

6-1 LOCKS AND KEY CONTROL. The security of any property or facility relies heavily upon physical locking devices. This is particularly true within the DOT where locks are, perhaps, the most frequently utilized physical security safeguard. It must be understood, however, that locks, although basic to any security system, are primarily a delaying device and seldom of much value in and of themselves. Locks, therefore, must be supplemented, where appropriate, with other security and protection devices and combined into the total security system. In many instances improper selection or application of locking hardware has minimized the effectiveness of a locking system. It is essential, therefore, that an assessment of all locking hardware, door frames, and jambs be included in any physical security survey.

6-2 TYPES OF LOCKING HARDWARE. Locking hardware varies greatly in appearance as well as function and application. The following describes the most prevalent locking hardware currently in use or available to DOT facilities.

a. Key Locks. Key locks include mortise cylinders, rim cylinders, padlocks, cylindrical locksets, tubular locksets, etc. This type of locking hardware is limited in that most key locks can be picked by an expert in a few minutes. There are, however, a number of high-security key padlocks available on today's market which are ideally suited for securing bulk storage areas containing sensitive and/or high value items and equipment (Figure 6-1). While the possibility of lost keys tends to minimize their effectiveness, this can be offset somewhat through the use of interchangeable cores.

b. Manipulation-Resistant Combination Locks. A manipulation-resistant lock is so designed that the opening lever does not come in contact with the tumblers until the combination has been set. This type of lock furnishes a high degree of protection for classified or sensitive material. (See Chapter X for approved combination locks.)

c. Interchangeable Cores. The interchangeable core system utilizes a type of lock with a core that can be removed and replaced by another core using a different key. Its main features include:

(1) Cores may be quickly and easily replaced.

(2) All locks can be keyed into an overall complete master-keyed locking system.

(3) Economical due to reduction in maintenance costs and new lock expense.

(4) System is flexible and can be engineered to the facility's needs.

(5) Simplifies recordkeeping.

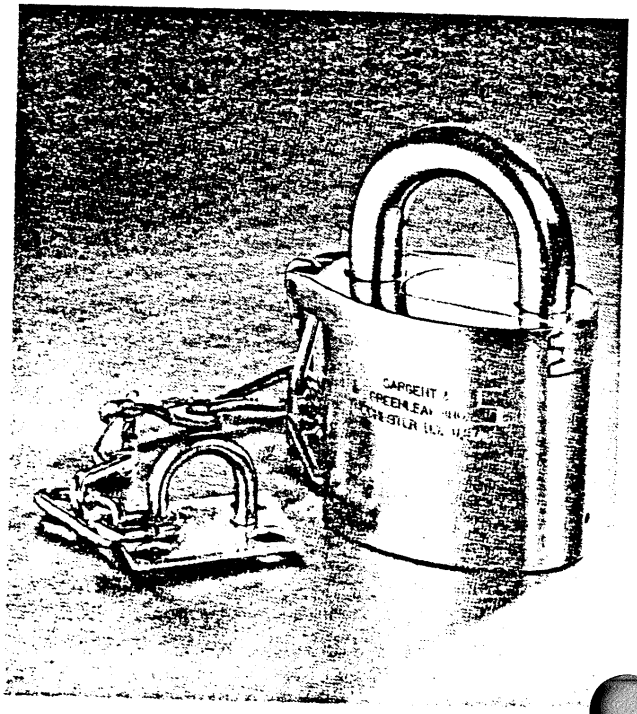
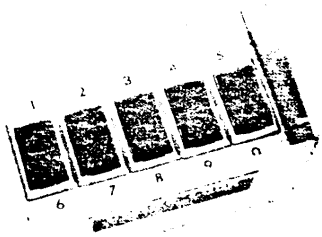
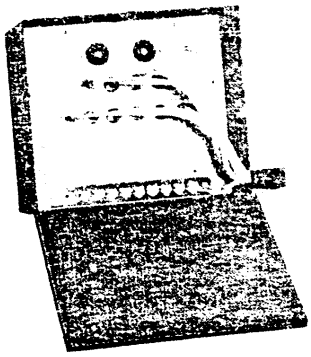


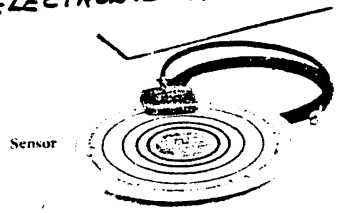
FIGURE 6-1. HIGH-SECURITY LOCKS

FINGERPRINT ACCESS DEVICE



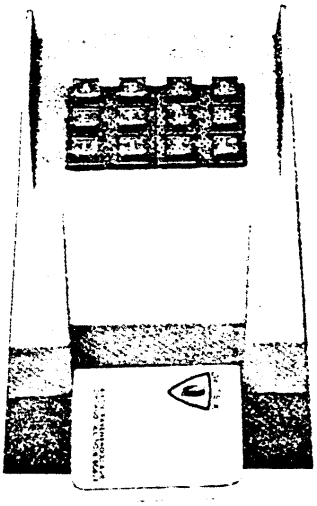


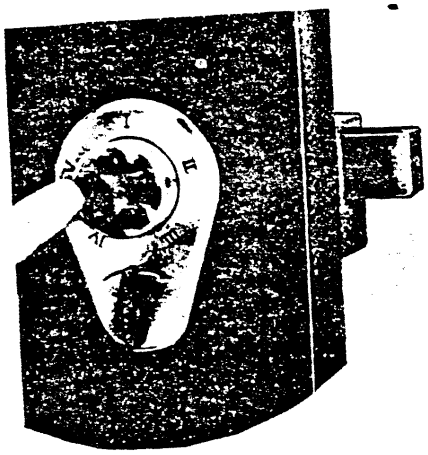
ELECTRONIC ACCESS CONTROL DEVICE

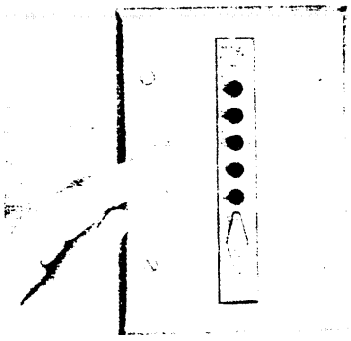


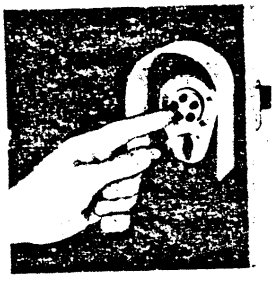
ELECTRONIC SENSOR CONTROL DEVICE

Encoded card/combination control device









pushbutton combination spring latch lock with spyproof shield.

STANDARD 3 GANG FLUSH DEVICE PLATE MOUNTING.

MECHANICAL CONTROL DEVICE

FIGURE 6-2. ACCESS CONTROL DEVICES

d. Electro-Mechanical Door Devices. There are a number of such devices available which operate by a push-button combination. Chief advantages are: low cost of lock, easy installation, combination easily changed, no key problem, simple to operate, affords relatively high degree of security. Depending on the model selected, the number of buttons ranges from 5 to 10. Some models also have "time penalty" and error alarm features and can be tied-in to an existing alarm system (Figure 6-2).

e. Other. Numerous locking systems are available, and others are being developed which use neither keys nor combinations. These include locks which open when a coded card is inserted; others which open when a fingerprint (previously recorded in a memory bank) is placed on a glass plate; another type opens when a previously recorded voice speaks into a microphone. These locking systems should only be utilized after consultation with the servicing security element.

6-3 KEYS. The following are some of the different types of keys:

a. Operating keys - The keys that are in daily use to open locks.

b. Duplicate keys - Those which duplicate operating keys and are usually stored for use in an emergency (e.g., loss of a key, or absence of the holder of the operating key). They must be stored securely in a safe or other locked container.

c. Master keys - Those which open a series of locks. They are used only as a matter of convenience in carrying one key instead of numerous keys. They must be carefully controlled, and all markings removed which identify them as master keys.

d. Construction keys - The keys which open the locks installed on the doors during the construction phase at a facility.

e. Control keys - The keys which are used to remove the cores of locks for purposes of changing.

6-4 ISSUANCE AND CONTROL OF LOCKS AND KEYS. Of primary importance in the safeguarding of property and controlling access is a good lock and key issuance and control system. For effective control, accurate records should be maintained and periodic physical inspections and inventories made. The main principles to observe are:

a. Keys, coded cards, and push-button combinations should be accessible only to those persons whose official duties require access to them.

b. Combinations to push-button locks will be changed following the discharge, suspension, or reassignment of any persons having knowledge of the combination, and at such other times as deemed appropriate.

c. Issuance of keys will be kept to a minimum and retained under constant key control supervision. The following measures are recommended for the control of keys:

(1) Unissued keys should be stored in a locked container when not in use.

(2) Access lists for persons authorized to draw keys should be maintained in the key storage container.

(3) Key containers should be checked periodically and all keys accounted for.

d. Locks should be changed depending on the sensitivity of the protected area and/or the relation of unaccounted for keys.

6-5 KEY CONTROL RECORDS. Key control records should be maintained on all key systems. Accountability can be maintained by records, key control cards, and key control registers. These records will include at least the following information:

a. Combination code for interchangeable cores.

b. Total number of keys in the system.

c. Total number of keys by each keyway code.

d. Number of keys issued.

e. Number of keys on hand.

f. Persons to whom keys have been issued.

Inventories of keys should be conducted annually. Requests for issuance of new, duplicate, or replacement keys should be approved or monitored by the official responsible for key control.

6-6 KEY CONTROL OFFICIAL. A key control official shall be appointed for every DOT facility having control over its own locking system. This official

should be concerned with the supply of locks and how they are stored; the handling of keys; records maintenance; investigation of loss of keys; inventories and inspections; custody of master keys and control keys, if applicable; regulations concerning locks and keys at the facility; maintenance and operation of the facility's key depository; and lastly, the overall supervision of the key program at the facility. The key control official should maintain a permanent record of the following:

a. Locks by number, showing:

(1) Location of each lock;

(2) Key combination, i.e., pin lengths and positions;

(3) Date of last key change.

b. Keys by number, showing:

(1) Location of each key;

(2) Type and key combination of each key;

(3) A record of all keys not accounted for.

6-7 RECOMMENDED LOCKING SYSTEM. Each DOT facility should have a master-keyed locking system, with all locking hardware supplied by the same manufacturer. This system should include locking hardware of the medium or heavy duty type, and interchangeable cores to permit maximum flexibility.

CHAPTER VII

7-1 GUARDS. If properly selected, trained and supervised, a guard force can be an effective and useful component of a facility's physical security program. If such qualities are lacking in the guard force, it can work to the detriment of the program and detract from the effectiveness of other protective measures. Physical protective devices, physical barriers and intrusion detectors depend ultimately on human intervention for their success or failure. Where there is a need for full time guards, they will be either Federal Protective Officers provided by the Federal Protective Service of GSA or guards furnished by a private company under contract to GSA or DOT or DOT employees.

7-2 DUTIES. Guard duties consists principally of the following:

a. Enforce the personnel identification system.

b. Observe and patrol designated perimeters, areas, structures, and activities of security interest.

c. Detain persons attempting to gain unauthorized access to the facility.

d. Conduct interior patrols of rooms, buildings and other structures of security interest during other than normal working hours.

e. Enforce the established system of control over the removal of property from the facility.

f. Respond to protective alarm signals or other indications of suspicious activities.

g. Respond to situations affecting the security of the facility (including fires, accidents, internal disorders, etc.).

h. Safeguard personnel, information, materials, and equipment.

i. Prepare and submit written incident reports to the appropriate security office and otherwise keep officials apprised of the security conditions within the facility.

7-3 NEED FOR GUARD FORCE. The need for a guard force is dependent upon many factors; such as:

a. Size, location and configuration of the facility, including topography.

b. Mission of the facility and its criticality.

c. Vulnerability to theft or damage of material, data and equipment.

d. Population of the facility and volume of pedestrian or automobile traffic.

e. Availability of funds.

Additionally, the need for a guard force is less during working hours than during non-working hours. During working hours, the presence of employees at their work stations can, to a large measure, deter the entry of unauthorized persons.

7-4 SELECTION. Where GSA provides the protective service at a DOT facility, basic reliance must be placed on GSA to assign qualified officers to perform the assigned duties. The DOT security element concerned should, however, maintain an overview of the officer's performance and notify the appropriate office within GSA whenever instances are noted of non-performance of duties. Where contract guards are utilized at a DOT facility, the DOT security element concerned has a more decisive role to play in the selection process, particularly if the contract is to be awarded and administered by a DOT activity. Irrespective of who awards the contract -- DOT or GSA -- it is essential that the security element participate directly in the development of the contract specifications setting forth the basic qualifications for the guards. The security element should closely monitor the performance of the contract and work closely with the management officials of the guard company in insuring compliance with the terms of the contract and the related guard orders. Where the contract has been awarded by GSA, any discrepancies that are observed should be promptly reported to the GSA Contracting Officer Technical Representative who, in turn, can refer them to the guard contractor for remedial action.

7-5 QUALIFICATIONS. Most of the qualities desired in guards are developed through training and become instinctive through experience. In addition to being able to comprehend and comply with written and oral instructions, some of the other qualities that guards should possess are:

a. Alertness. This quality, more than any other, will determine the effectiveness of a person assigned to security force duties. Alertness can be achieved only by keen watchfulness and by diligent application to the requirements of the patrol or post. Technological advancements in communications equipment and protective alarm systems enhance the effectiveness of security forces; but nothing can be substituted for the alertness of security force personnel.

b. Judgment. Sound judgment is more than the application of common sense; it is the power of arriving at a wise decision. Each man must develop the ability to observe, compare, and contrast. Guards, however, should be trained to call security headquarters for instructions when in doubt as to a situation.

c. Physical Fitness. Many security duties are physically demanding, such as conducting foot patrols in and around large, extensive facilities and responding quickly to alarms and requests for assistance. Therefore, guards need to be in good general health and have no physical defects that would hamper them in the performance of their duties.

d. Tactfulness. The ability to deal tactfully with others is a quality desired in guards. Security personnel must be able to give instructions clearly, concisely and firmly, but without arrogance.

e. Self-Control. Security duty presents situations which require not only sound judgment and tact but also self-control. No matter what the degree of provocation or what stresses and strains a guard may be subjected to, he must be able to retain his composure and react in a calm, mature manner.

7-6 SPECIAL REQUIREMENTS.

a. As a general rule, guards should only be required to have security clearances when, in the performance of their assigned duties, they may have occasion to have access to classified material. Under that criteria, guards who, for example, conduct security checks of classified storage containers after non-duty hours, or who control access to controlled areas containing classified material, would have a valid need for a security clearance. The level of the security clearance would be determined by the highest category of classified material involved. The important thing is that security clearances are not requested indiscriminately, not only because clearance actions are costly and time consuming, but also because of the adverse affect it may have on the contract performance due to the unavailability of cleared guards.

b. Contract guards should not be required to be armed unless there are compelling reasons for doing so. In the event it is determined that it is essential for the contract guards to be armed, then the requirements of DOT 1620.1A, Use of Weapons by DOT Personnel, should be incorporated into the provisions of the contract.

7-7 MANPOWER REQUIREMENTS. After the desired number of actual guard posts has been determined, the approximate number of guard personnel needed can be calculated as follows:

Continuously manned post requires 168 man-hours per week (1 man, 7 days, 24 hours). Compute the total number of man-hours per week for all continuously manned posts and divide by 168. This gives the number of fixed posts. Ascertain the average number of days of annual leave and sick leave that will probably be required. From the following table, find the "number of guards per posts required" appropriate to the average leave anticipated. Multiply this figure by the number of posts required.

If average number of days annual and sick leave anticipated per man is:	Number of guards per posts required (40-hour week)
0 (basic)	4.2
20	4.55
25	4.6
30	4.7
35	4.85
40	4.96

EXAMPLE

Post #1	1 man, 24 hours, 7 days
Gate	1 man, 10 hours, 5 days
	1 man, 2 hours, 5 days TOTAL 228 hours
Post #2	1 man, 24 hours, 7 days TOTAL 168 hours
Post #3	2 men, 16 hours, 7 days 1 man, 8 hours, 2 days TOTAL 240 hours

The formula indicated does not reflect man-hours required for training, special details, and miscellaneous assignments. If these special assignments are bonafide security responsibilities, and the man-hour requirements are fairly consistent and can be guaged on the basis of "averages" indicated by past experience, appropriate adjustment of guard force can be made with little difficulty. However, if such requirements are intermittent or generally of limited duration, consideration should be given to the use of overtime or temporary curtailment or doubling-up of posts. One individual shall be placed in charge of each shift. Changes of shifts should occur before peak periods of activity in the normal operation of the facility.

7-8 GUARD ORDERS.

a. Instructions to the guard force should be issued in writing and contain the basic requirements as determined by the DOT security element. These instructions are normally in the form of General, Special and Temporary Orders, and should be clearly worded to include all the responsibilities of each assignment. They should be specific as to the action to be taken based on each and every type of emergency situation. They should be reviewed at least monthly to be certain they are current. Categories of instructions are:

(1) General Orders. Orders which concern the guard force as a whole and are applicable at all posts and patrols are General Orders. They will cover such items as wearing of the uniform, reporting for duty, report writing, etc.

(2) Special Orders. Orders which pertain to the responsibilities of a particular post or patrol are Special Orders. Each post or patrol should have Special Orders issued concerning the location, duties, hours manned, etc.

(3) Temporary Orders. Orders which are issued for a short period covering a special or temporary situation fall into this category. If it can be predetermined, such orders should indicate the period of time for which they are valid.

b. Guard Orders should be prepared by the DOT security element concerned or prepared by GSA or the guard contractor based on the input received from the DOT security element. Likewise, temporary orders would be prepared by the security element, covering such things as admitting non-employees to the facility during security hours, arranging for certain areas to be unlocked for a specific purpose, etc. The essential thing is that the orders be concise, easily understood and discussed with the guards to insure that they are interpreted correctly.

The only exception to this policy would be when the security element has delegated the responsibility of preparing the guard orders to the management of a faciltiy, provided that the guard orders are subject to review and approval by the security element.

CHAPTER VIII

8-1 INTRUSION DETECTION SYSTEMS.

a. Alarm systems are designed to alert security personnel to an actual or attempted intrusion into an area. The use of these mechanical and electronic warning systems has proven beneficial in many situations; however, individuals responsible for physical security planning must be aware of the advantages and limitations of these devices.

b. There are a variety of commercially manufactured devices available which are designed to detect approach or intrusion. Other more sophisticated devices are continually being developed. Certain types of systems are suitable only for exterior protection, while others are suitable only for interior uses. All have weak points by which their functioning can be minimized or even completely interrupted.

c. Intrusion detection devices may be used to supplement or supplant the security force. They are designed to detect intrusions or attempted intrusions, not to prevent them. The best intrusion detection system is ineffective if appropriate security procedures and quick response is not an integral part of the overall security plan. It is the response force which provides the real protection to any sensitive area.

8-2 PLANNING A SECURITY ALARM INSTALLATION. Security alarm equipment is normally classed into three general categories:

a. Point or object protection;

b. Area or space protection; and

c. Perimeter protection.

It is with the combination of two or more of these components that an electronic security system achieves the desired depth of protection. The difficulty of attempting to overcome one system only to be faced with another, perhaps even more effective, is both a psychological and a physical deterrent.

8-3 FEASIBILITY ANALYSIS. The following factors need to be considered in determining the need for an alarm system:

a. Mission of the facility.

b. Criticality of the facility.

c. Vulnerability of the facility.

d. Accessibility to intruders.

e. Location of the facility and locations of areas to be protected.

f. Construction features.

g. Hours of operation.

h. Availability of other forms of protection.

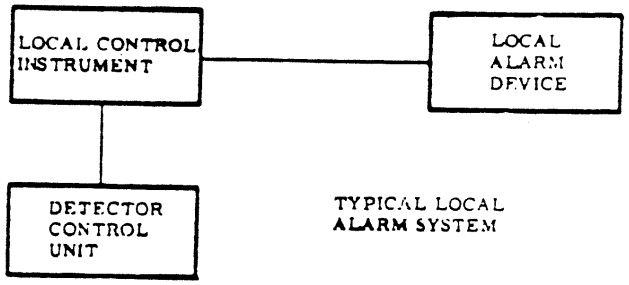
i. Initial and recurring cost of alarm system weighed against the cost of losing materials or information.

j. Response capability.

k. Savings in manpower and money over a protracted period of time.

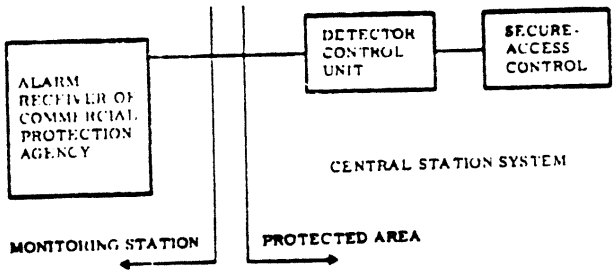
8-4 ALARM REPORT SYSTEMS. Alarm and communications systems are closely allied in any comprehensive protection system. Telephone and radio communications are so common in everyday usage that their adaptation to a protective system poses few new problems. An alarm system is simply a manual or automatic means of communicating a warning of potential or present danger. Types of alarm systems include the following:

a. Local Alarm System - A system in which the protective circuits in the secured area are directly connected to a sound producing apparatus such as a bell or siren. The sounding device must be mounted on the exterior of the building containing the secured area. The bell must be fully protected against weather and wilful tampering, be connected to the control panel by tamper-proof cable, and be audible for a distance of at least 400 feet.

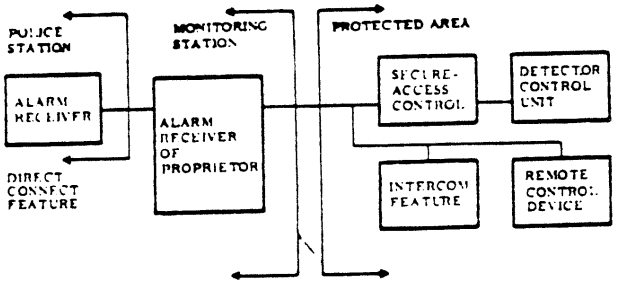


TYPICAL LOCAL ALARM SYSTEM

b. Central Station Alarm - A system in which the secured area is connected to an alarm panel in a centrally located station via a pair of leased telephone wires. Upon receiving an alarm, the monitoring station will dispatch its guards to the location of the secured area. Alarm installations of this type should only be utilized when the response time is no more than ten minutes.



c. Proprietary Alarm - An installation similar in most respects to a Central Station type, except that the alarm panel is located within a manned guard room on the premises. A proprietary guard force operates the system and responds to all alarms. A modification of the proprietary system is where the alarm monitor is installed in a nearby police station via a pair of telephone wires.



PROPRIETARY SYSTEM WITH DIRECT CONNECT

8-5 CHARACTERISTICS OF ALARM SYSTEMS.

a. Essential characteristics of an alarm system include the following:

(1) A detection unit or detection components located at the protected area and designed to initiate an alarm upon intrusion of a human into the area, or approach of a human to a protected object.

(2) Signal transmission lines which conduct the alarm signals from the protected area to a central annunciator panelboard which should be constantly monitored.

(3) A central annunciator panelboard containing the electronic components which announce, by both visible and audible signals, intrusion into protected areas and the specific structure or location involved.

(4) Fail-safe features which give an alarm signal at the annunciator panelboard when abnormal operating conditions preclude the alarm system from functioning properly as well as back-up power source.

(5) Features which make it less vulnerable to tampering or circumvention. Such features should include capability of concealment and difficulty of neutralization.

8-6 SECURITY OF ALARM SYSTEMS. There are two basic means of providing security for alarm systems. First, security is provided by built-in technological security measures, i.e., as more technology (sophistication) is built into a system, more technology is required to breach, or defeat the system. However, as more technology is built into a system, the cost of the system and the cost of maintenance increase accordingly. Second, security is provided by the use of physical security measures, i.e., the height of reporting lines on poles or the depth they are buried in the ground, control of access to the system equipment, etc. Physical security measures should be applied in inverse proportion to the built-in technological security measures of the system. The ideal is to provide a balance between the built-in technological security measures and the physical security measures. The ideal balance is at the point where the breach or "defeat time" element of the system is achieved through the use of a combination of technological and physical security measures at the lowest costs.

8-7 PRINCIPLES OF OPERATION.

a. No one system is suitable or adaptable to every location and environment. The situations and conditions at the particular site to be protected determine which devices or systems are efficient and practicable.

b. Following are some of the basic principles upon which these devices operate:

(1) Breaking of an electric circuit.

(2) Interruption of a light beam.

(3) Detection of sound.

(4) Detection of vibration.

(5) Detection of motion.

(6) Detection of capacitance change due to penetration in an electronic field.

8-8 TYPES OF EQUIPMENT. Each class of equipment deserves a more lengthy treatment than will be presented here. For conciseness, only the salient features are outlined.

a. Electrical/Mechanical Premise Alarm - Consists of the protection of all doors, windows or other accessible openings into the protected area by means of contact devices, switches, and metallic foil tape. In some instances, wired wood dowel screens are used to protect windows, transoms, or similar type openings, instead of the metallic foil. These are arranged to form a continuous closed circuit loop connected to alarm relays in a control cabinet located within the secured area. If an attempt is made to enter through one of the protected points, the circuit will be broken and set off the alarm.

Advantages:

(1) Relatively simple, trouble free system.

(2) Usually low cost installation unless dealing with complex type multi-pane windows or extended premises.

(3) May be adequate in low risk applications.

Disadvantages:

(1) Minimum grade of recognized protection. May be upgraded by addition of protective equipment applied to all openings, walls, floors and ceilings, at considerable increase in cost.

(2) Rather easily compromised. Unprotected soft walls or ceilings may be penetrated without disturbing alarm system.

(3) Little salvage value -- major cost of job is installation, not recoverable.

(4) Will not detect "stay behinds" until they leave premises.

b. Capacity Alarms - One of the most successful applications of electronic techniques in the field of security alarms is found in the class of equipment known by the name of "capacity alarms."

(1) Protected object acts as part of the capacitance of tuned circuit (as a capacitor or condenser). If a change occurs in the region of the protected object, such as the approach of an individual, there will be a change in the capacitance of sufficient magnitude to upset the balance of the system and cause an alarm. Capacitance alarms are universally used for point protection of specific objects requiring a high degree of security; i.e., safes, file cabinets, or other metallic storage containers. When applied to safes or files, the system is flexible and may be used to connect several safes or files in the same area to one system.

(2) Unlike space alarm systems, the protective field on the safe or file is usually kept down to a depth of not more than a few inches from the surface of the safe. This prevents unwanted alarms from authorized persons passing within a few feet of the safe without any intent of intrusion. Very close proximity, or contact with the protected object, will set off the alarm.

(3) The system may be connected to window or door grids of metallic tubing to provide protection for such openings. Antenna systems consisting of horizontally strung wires may be installed between the top of low partitions and the ceiling to form a protective security barrier in buildings having restricted areas and non-secured areas in close proximity. The application of transistorized circuits in the latest type of capacitance systems provides excellent stability in the equipment.

Advantages:

(a) Extremely flexible type of system -- may be used to protect safes, file cabinets, windows, doors, partitions; in fact, any ungrounded metallic objects within maximum tuning range of the system to be protected.

(b) Simple to install and operate.

(c) Provides an invisible protective field making it difficult to determine what is protected.

(d) High salvage value -- may be easily dismantled and reinstalled.

(e) Compact equipment size.

(f) High degree of security.

Disadvantages:

(a) Can only be applied to ungrounded equipment.

(b) Accidental alarm can occur if protected safe is carelessly approached by cleaners.

c. Photo-electric - The photo-electric cell, or electric eye, is a device customarily used in conjunction with other forms of alarm equipment. Its operation depends upon the interruption, or breaking of the beam of light between a projector and a light-sensitive receiver some distance away. When the light is cut off from the receiver, an alarm relay is actuated in a control cabinet within the secured area.

(1) Since white light is easily detected, infra red beams are preferable for security alarm installations. Although these have very low visibility, if located they may be compromised by introducing a substitute source of illumination which will permit penetration of the system with an alarm. The better systems overcome this problem by providing a modulated beam which must be synchronized with a corresponding pulse in the receiver. If the synchronized beam is interrupted or an attempt is made to substitute a foreign light source, an alarm will sound.

(2) Some electric eye installations employ mirrors to more efficiently utilize the capabilities of the equipment, providing more effective criss-cross pattern for better coverage. To prevent detection, mirrors and the projector-receiver combination should be concealed wherever practical.

(3) Photo-electric units are often combined with premise alarms to provide more satisfactory coverage of the secured area against penetration of unprotected walls or ceilings. In other instances they may be used to protect long rows of windows in lieu of window foil. Outdoors, special weather proof photocells may be used to protect gates, roadways, aircraft runways, or other locations where physical obstructions cannot be tolerated. Special environmentally controlled housing are used for outdoor or modulated systems.

Advantages:

(a) Covers open portals or driveways where no physical obstructions can be tolerated.

(b) Can increase effectiveness of premise alarms.

(c) Makes it difficult for persons concealed within the premises to operate without detection.

(d) Has high salvage value -- almost all equipment recoverable.

(e) May be used to actuate other security devices, such as cameras.

Disadvantages:

(a) Beams are of narrow cross-section and may be located and avoided by careful intruder.

(b) Substitute light sources have been used to defeat even modulated beam systems.

(c) Operates on 110 volts -- standby power supply.

(d) Transmitter, receiver, and mirror (when used) susceptible to being knocked out of alignment.

(e) Dusty, smokey atmospheres may deposit soot or dirt on lenses and mirrors causing failure.

(f) Exterior systems subject to interference from fog, heavy snow, snow drifts.

d. Space Type Alarms.

(1) The protection of an enclosed space can often be effectively achieved by use of a class of equipment identified as a space alarm. Such systems usually derive their operating principles from a phenomena known as the Doppler Effect. The best known type of system in this category is popularly called "ultrasonic" although it actually operates just within the upper limits of the audio frequency spectrum.

(2) The apparatus generates a train of high frequency sound waves which fill an enclosed area with a pattern of standing waves.

A sensitive receiver, connected to an electronic amplifier, picks up the waves; if they are of the same frequency as the sound emitted by the transmitter, the system will not sound an alarm.

(3) Any motion within the protected area will send back a reflected wave differing in frequency from the original transmission. This change in frequency will be detected, and amplified in the control unit, and the alarm signal will be activated.

(4) Since the system will detect all types of motion, it is essential that movements of any type, i.e., air currents, moving machinery, animals, or other possible disturbances be eliminated from the secured area. Large inductive or magnetic fields must also be kept away from the transmitters, receivers, and their connecting cables to prevent accidental alarms. Multiple transmitters and receivers may be operated from the same control unit for more effective coverage of large or broken areas. The system can only be used indoors.

Advantages:

(a) Provides effective security protection against intruders concealed within the premises.

(b) Protective field is not visible, therefore, it is difficult to detect the presence of, or to compromise the system.

(c) Reasonably flexible in its application to interior protection problems.

(d) Affords complete protection on premise installations, when supervisory contacts are used on all movable openings.

(e) High salvage value -- equipment may be removed and relocated if necessary.

(f) Portability in some models.

Disadvantages:

(a) May require reduced sensitivity to overcome possible disturbance factors in the secured area.

(b) May not detect very slow movements (slower than 4 steps in 4 seconds).

(c) Can be set off by loud external sounds, or building vibrations.

(d) May not detect penetration of walls behind large objects close to wall.

(e) Cannot be used in high sound absorbing area.

(f) Requires expert planning if installation is to have satisfactory results.

(g) Can be "heard" by some people -- very irritating to anyone with sensitive hearing.

e. Audio Systems (Space) - Even though these systems are in the space protection family, they should not be confused with ultrasonic systems. A sound system only "listens" to the protected area, it does not "fill" the area with any kind of waves.

(1) Audio systems, unlike ultrasonic, can tolerate air movement and other types of motion as long as the noise created is relatively low. Where fans or other noise-producing items are in a fixed part of the room, cancellation microphones located in close proximity to the noise-producing component may be used to nullify only that specific noise(s).

(2) The sensitivity of these systems can be adjusted to detect a very small amount of noise; however, this will in most installations cause nuisance alarms. The sensing circuit is a "stepper type;" each short noise will cause one pulse or step -- if extended noise is heard, more than one pulse is registered. Most systems are adjustable in sensitivity, alarming between three and ten pulses. An individual wearing tennis shoes could probably walk through the protected area without causing an alarm.

Advantages:

(a) Can often use existing intercom or speaker systems as detector microphones.

(b) Covers large volume.

(c) Inexpensive installation with existing sound systems.

Disadvantages:

(a) Does not provide "perimeter" protection.

(b) Susceptible to outside noises.

(c) Should not be used in non-reverberant areas.

f. Vibration Detectors - The detection of vibration caused by an attack upon the walls, ceiling or floor of a protected structure is the primary function of the audio alarm system. A microphone and amplifier is adjusted so that ambient noises or normal sounds will not trip the alarm. However, noises about this level will be amplified with sufficient power to actuate the alarm relay. Where ambient noise is too high, contact type detectors can be used in place of microphones. These contact detectors do not respond to the airborne sounds, but are sensitive to vibrations within the wall or structure upon which they are mounted. These detectors are not of the "one shot type;" they have the same capabilities as microphones since they too transmit vibrations to the accumulator circuitry.

Advantages:

(1) Easy installation - relatively few parts required.

(2) Very effective complete protection for vault structures.

(3) Can be used as an audio monitor as well as alarm in some applications.

(4) Contact detectors can be used when ambient noise levels are too high.

(5) High degree of salvage - equipment may easily be removed and reinstalled.

(6) Very flexible - may be used to cover large or small areas with small cost differentials.

Disadvantages:

(1) Sensitivity to all sounds makes the units ideal only for locations with low ambient sound levels.

(2) Tube type models require frequent sensitivity checks.

(3) Must be combined with other equipment to protect movable openings into secured area.

g. Radar or Microwave Type Systems - Since the advent of radar, there have been many attempts to devise a space alarm system using radar techniques. The principles employed closely parrallel the operation of the ultrasonic system with some notable exceptions. Radio waves are highly penetrating and are not easily confined within a closed area such as a room or building. A train of waves is produced which are partially reflected back to the antenna. If all objects within the range are stationary, the reflected waves return at the same frequency; if they strike a moving object, they return at a different frequency. The difference in the transmitted and received frequency appears as a low frequency signal which is detected and used to trip an alarm relay. The area covered by the radiation field may be controlled to some extent by the number and placement of antennae. Sensitivity is controlled by adjusting the amplifier. The radar units are generally used to protect interior areas, and are therefore classed as space alarms.

Advantages:

(1) Equipment is compact and may be rapidly installed.

(2) Good coverage provided if antennae are placed properly.

(3) Radiation field difficult to detect so that intruder may not know when he has tripped alarm.

(4) Not affected by air currents, noise, light, or sound.

(5) High salvage value.

Disadvantages:

(1) Coverage is not easily confined to desired security areas; may be accidentally tripped by persons or vehicles outside of protected area.

(2) May be accidentally tripped by other radio transmitters operating at frequencies close to the generated frequency.

(3) Stability of operation still questionable.

(4) Requires 110 volt power source for electron tubes.

(5) Tube replacement expensive.

CHAPTER X

10-1 STORAGE EQUIPMENT. Many types of containers are being used within the Department of Transportation to meet the storage requirements established by DOT 1640.4, Classification, Declassification and Control of National Security Information. This Chapter is intended to assist facilities in the proper selection and use of storage containers. While many of the containers described in this Chapter are designed primarily for the storage of classified material, such containers could also be used for such purposes as protecting monies, drugs, weapons and sensitive/proprietary data.

10-2 INTERAGENCY ADVISORY COMMITTEE ON SECURITY EQUIPMENT. Progress in the security container field has been advanced by a program initiated during 1954 under the supervision of the General Services Administration (GSA), assisted by the Interagency Advisory Committee on Security Equipment of which the Department is a member. This program has resulted in the development of Federal specifications for security equipment, and has provided for the incorporation of approved equipment into the Federal Supply Schedule.

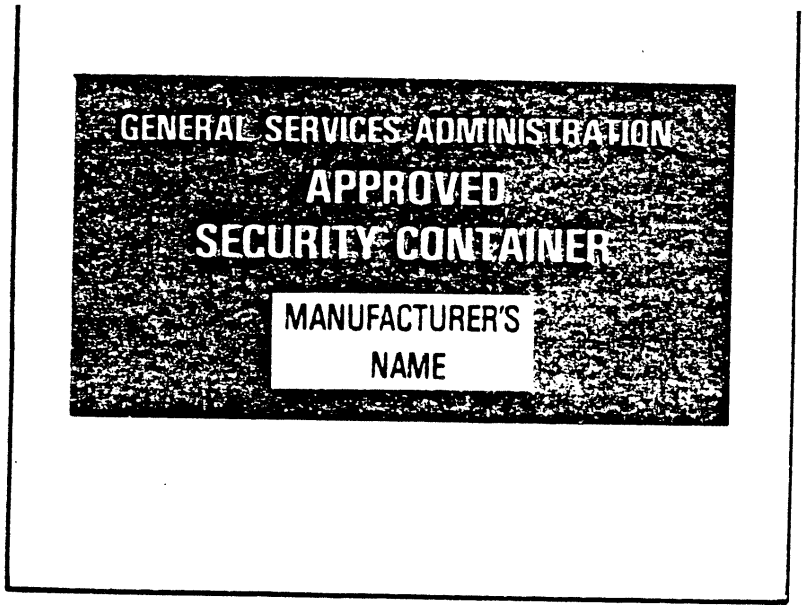
10-3 SECURITY FILING CABINETS.

a. Security filing cabinets are not identical with safes although both have locking devices. A safe is used to store items of monetary value and security cabinets are designed primarily to store classified material. Containers designed as a security filing cabinet have been specifically developed and approved for the storage of classified material and bears such a label (Figure 10-1).

b. DOT 1640.4 specifies that only security filing cabinets that have been approved by the Federal Government shall be procured whenever new equipment is required; and further, it prohibits modification of existing filing cabinets to a lockbar/padlock variety when such a modification is intended to provide a means for the storage of classified material. It is intended that this requirement will eventually result in the replacement of all nonapproved containers.

10-4 CLASSES OF APPROVED SECURITY FILING CABINETS.

a. Specifications have been developed for seven classes of security containers (classes 1, 2, 3, 4, 5, 6 and 8). However, only Classes 1, 5 and 6 are now available on the Federal Supply Schedule.



Label Required for Security Cabinets.

TYPES AND APPLICATION OF INTRUSION DETECTION DEVICES

Systems	Basis of activation	Application	Maintenance supervision problems	Nuisance alarms	Rating
Audio	Sound	Interior only (for vaults and low sound level areas).	Regular inspection to replace inoperative parts.	Frequent (from extraneous sounds).	Not as reliable as ultrasonic.
Sonic	Movement	Interior only.	Same as above	Few.	More reliable than audio.
Ultrasonic	Movement	Interior only.	Same as above	Few.	More reliable for protection of rooms.
Microwave	Movement	Interior only.	Same as above	Few.	Most reliable within patterns set by antennae.
Electro-mechanical	Breaking of electric circuits.	Interior only (doors, windows, skylights, ventilators, etc.).	Same as above	Few (window tape may break).	Affords minimum protection for buildings and rooms.
Electro-magnetic (interior)	Movement	Interior only (metal cabinets and safes).	Same as above	Few	Reliable for metal safes and cabinets.
Electro-magnetic (exterior)	Movement	Exteriors only (perimeters and also can be attached to side of building).	Same as above. Also to remove snow, ice, and debris from fence.	Many	Best device developed for fence line security
Photoelectric	Interrupting light beam	Interior and exterior (rooms, halls, gates, and perimeters).	Same as above. Also to clean transmitter and receiver.	Interior (few), exterior (many) (due to fog, rain, birds, etc.).	Interior: reliable when beams are crisscrossed for short distances. Exterior: gates and short distances only.

8-9 LINE SUPERVISION.

a. An alarm system is no better than the security of the lines that transmit the signal from the protected area to the monitoring station. These lines must be sensitive enough to cause an alarm signal in the event of tampering. An alarm system may be defeated by an intruder regardless of the effectiveness of its triggering mechanism if the signal line is not functioning properly. Lines may be made ineffective by an intruder who has sufficient knowledge of electricity, and the necessary equipment to adjust the resistance in the lines.

b. Manufacturers of the best commercial alarm equipment incorporate in their annunciator panels two relays, designated as the underload and overload relays. The purpose of the underload relay is to detect any appreciable drop in line current while the overload relay is intended to detect a substantial increase in current. However, if carefully accomplished, the line defeating method mentioned in paragraph a. above will not disturb either of the two relays.

c. Signal line tampering may be detected by assuring that a circuit has low line tolerance. For example, an alarm may operate on 20 milliamperes of line current. If the overload relay is set to drop out when the line current exceeds 30 milliamperes and the underload relay will drop out at 10 milliamperes, the line tolerance is said to be 20 milliamperes. Most standard alarm circuits have line tolerances ranging from three milliamperes (for storage vault installations) to 30 milliamperes (for many window foil and door switch protected rooms). Systems having line supervision on tolerance in the milliampere range can be defeated with little difficulty. In order to be effective, line supervision must not exceed 25 microamperes.

d. If signal lines for alarm systems installed at important facilities extend outside protected areas, cognizance should be taken of their vulnerability to tampering, and where feasible, microampere line sensitivity should be provided.

e. The need for constant electronic or other type surveillance of transmission lines must be emphasized to insure awareness of security personnel that this is normally the weakest link in the system. Emphasis must also be placed on the necessity to maintain records of nuisance alarms, and on continuing maintenance to insure proper operation of the system at all times.

CHAPTER IX

9-1 DESTRUCTION EQUIPMENT. DOT 1640.4 provides that classified material may be destroyed by burning, pulping, pulverizing, shredding or chemical processing (e.g., acetone), provided the destruction is complete and reconstruction is impossible. Generally, it is adviseable to burn classified material whenever possible since this is a positive and complete method of destruction and disposition of the ash usually constitutes no problem. Since combustion is relatively complete, and most of the products of combustion go up the stack in a gaseous state, there is very little fine ash left in proportion to the volume burned. Pulpers, pulverizers and shredders perform with varying degrees of effectiveness; however, with each of these processes the bulk residue may create a problem of storage and disposition. It is the intent of this Chapter to provide information to assist in the selection of equipment which will suffice not only for the destruction of classified material but also for the destruction of personal data falling under the Privacy Act of 1974, or other sensitive/proprietary information. The headquarters security element should be consulted before destroying classified material by methods other than those listed above (e.g., melting, decomposition).

9-2 INCENDIARY DEVICES. Incinerators can destroy virtually all mixtures and most configurations of classified materials that require destruction. However, all General Services Administration contracts for the procurement of incinerators through the National Supply System were cancelled on June 30, 1973, based on the Environmental Protection Agency's discontinuation of an incinerator testing and certification program. The Clean Air Act (42 USC 1857), as amended, has greatly restricted burning and, in some areas, it has also been prohibited by State or municipal legislation. Since pollution control criteria may vary between Federal, State, and local jurisdictions, it is recommended that local officials be consulted before purchasing an incinerator.

9-3 SHREDDERS. When using shredding machines, special attention must be given to the residue to insure that it cannot be reconstructed (Figure 9-1).

a. Shred Criteria. Shredding machines should produce residue no greater than the following:

(1) Strip-shredding. A strip-shredding machine must cut the material to be destroyed into shreds no greater than 1/32 inch in width.

(2) Cross-cut-shredding. A cross-cut-shredding machine must reduce the residue to shreds no greater than 3/64 inch in width and not more than ½ inch in length.

b. Added Precautions. Some precautions that should be observed are:

(1) The feed tray should always be used when shredding; otherwise, shreds ranging up to ¼ inch in width may result from the paper running to the outside edges of the cutter where no shredding action occurs.

(2) Paper should be placed through the machine in such a manner that the lines of print are horizontal in relationship to the cutter blades.

(3) Microfilm should not be destroyed in shredding machines except as a preliminary measure to more complete destruction by burning.

c. Application. The ability to destroy paper in shredders is normally limited to a maximum of two to five sheets at a time (depending on the type of paper), two Automatic Data Processing (ADP) cards inserted side by side, double sheets of carbon paper, and other similar light loads.

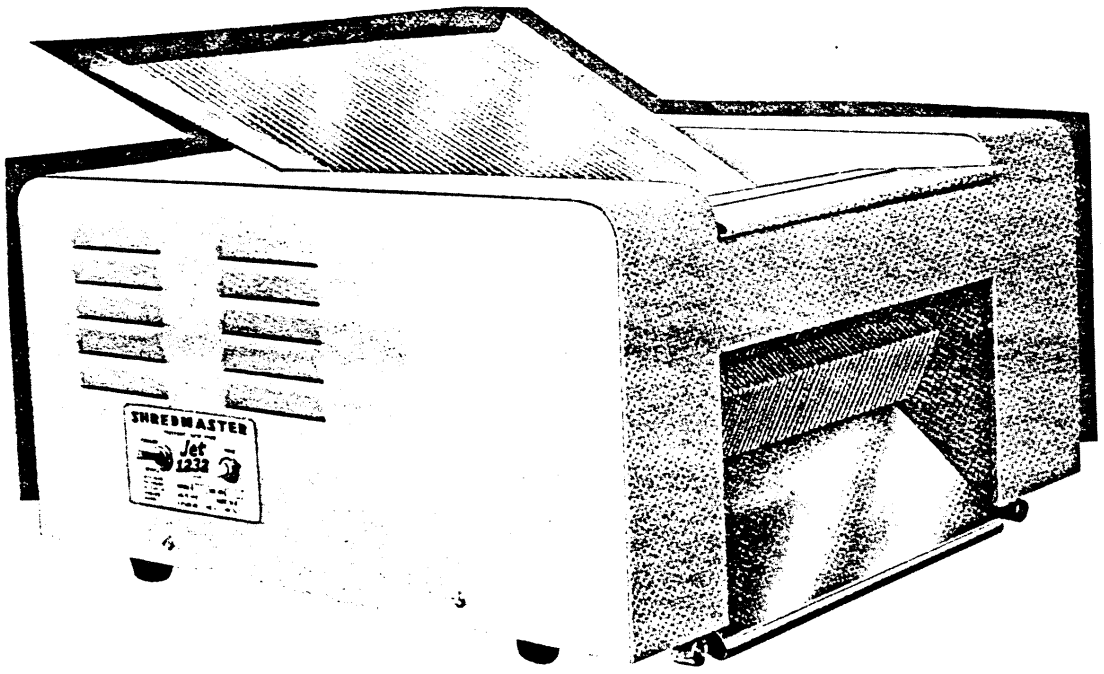
9-4 DISINTEGRATORS/PULVERIZERS. The Interim Federal Specifications which governs the manufacture of classified material pulverizing equipment listed on the Federal Supply Schedule requires a security screen with an aperture size no larger than 3/32 of an inch. This size security screen insures that reconstruction of the residue is not possible; but the aperture size may increase through wear, and the screen should be examined periodically and replaced if the aperture size is found to be larger than 3/32 of an inch (Figure 9-2).

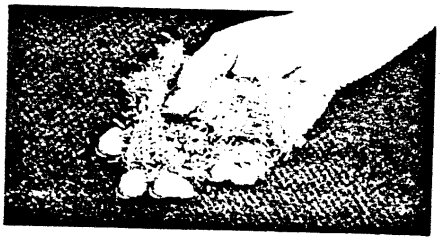
9-5 RECOMMENDATIONS. In selecting new destruction equipment or determining whether to update existing equipment, the following factors should be evaluated for cost and effectiveness:

a. Measures of Destruction System Effectiveness.

FACTORS	EVALUATION CRITERIA
(1) Security	Does the system, its location, and its operating procedure minimize the possibility that classified information could be compromised? Consider adequacy of the screening, inspection of interior, examination of residue, clearing of jams, physical security of destruction equipment, etc.

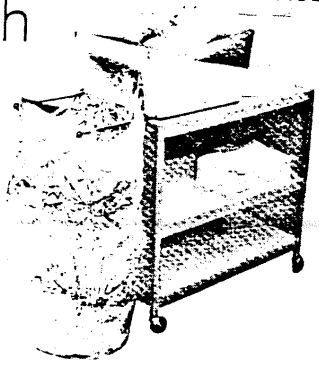
FACTORS	EVALUATION CRITERIA
(2) Safety	Are safety procedures adequate?
(3) Environment	To what extent, if any, does operation of the equipment contribute to pollution of the air, water, or land?
(4) Reliability	How many problems could disable the system or degrade performance, and what are their possibilities of occurrence? How long would it take to correct the various problems? Consider loss of required utilities.
(5) Local Disturbance	Does noise distract operators or others? Is system operation, including residue disposal, dusty or messy?
(6) Flexibility	Can the largest and the smallest anticipated requirements be met without lengthy storage or prolonged operation?
(7) Simplicity	Is the system easy to operate and maintain?

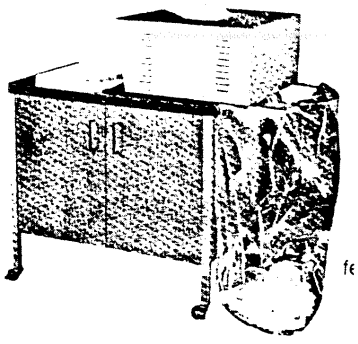


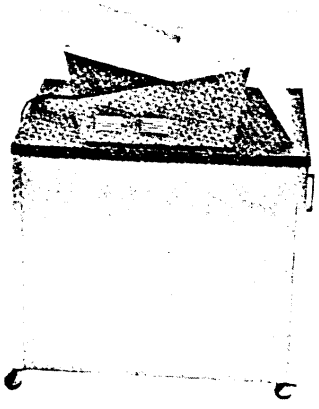


1/32" width by 1/2" length
(1/64" tolerance)

DESK-TYPE MODEL







CABINET TYPE MODEL

FIGURE 9-1. SHREDDERS

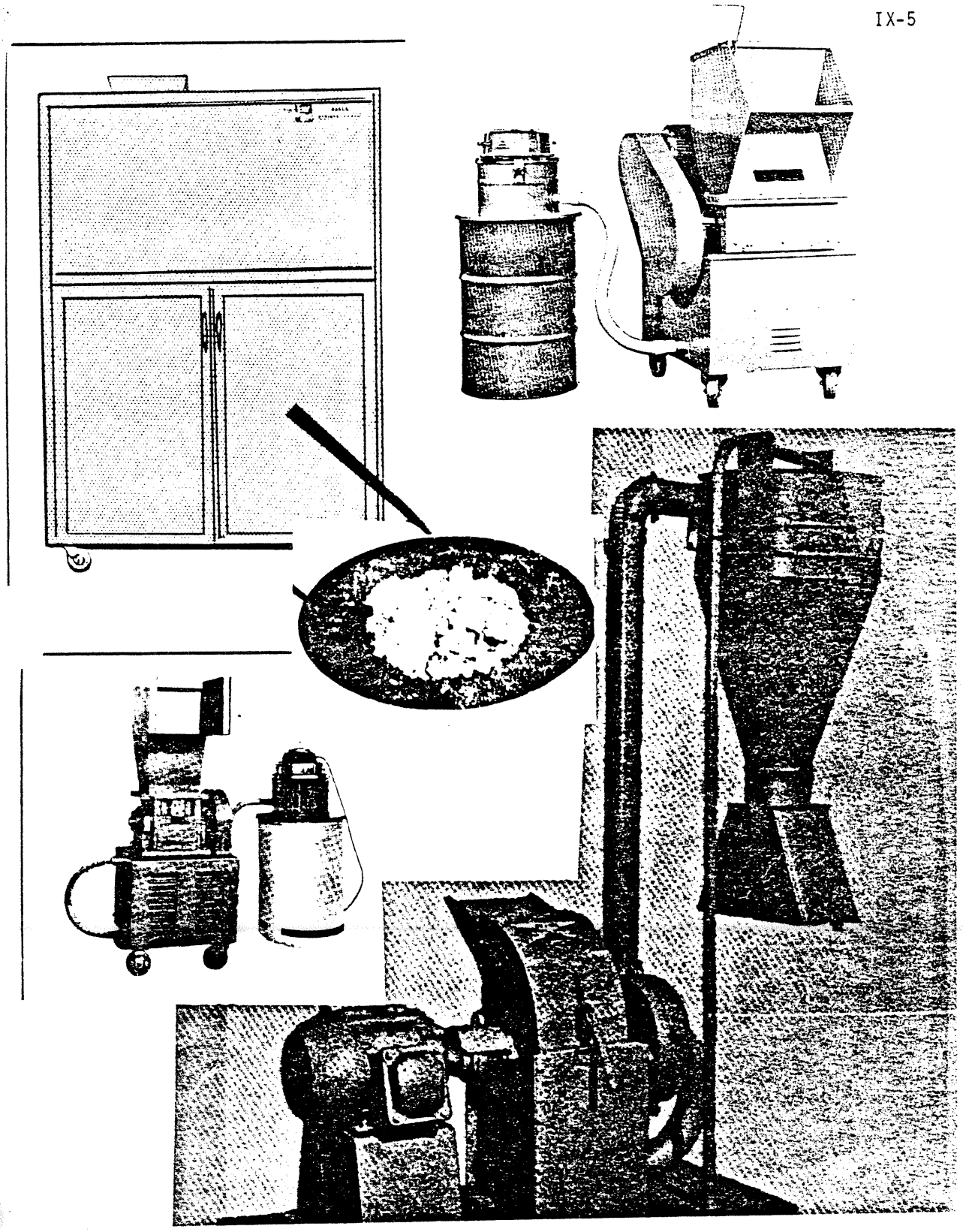
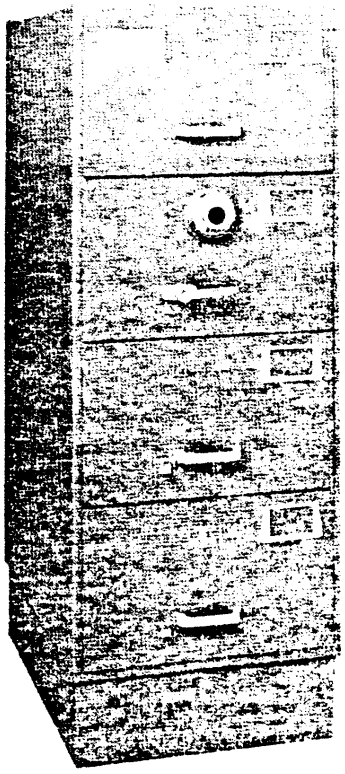
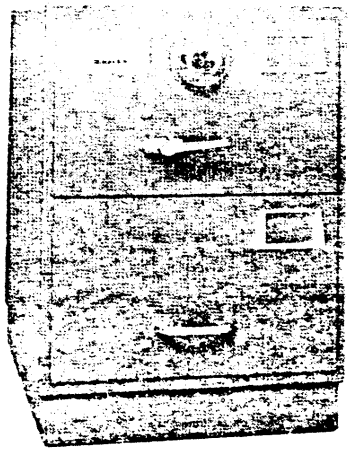
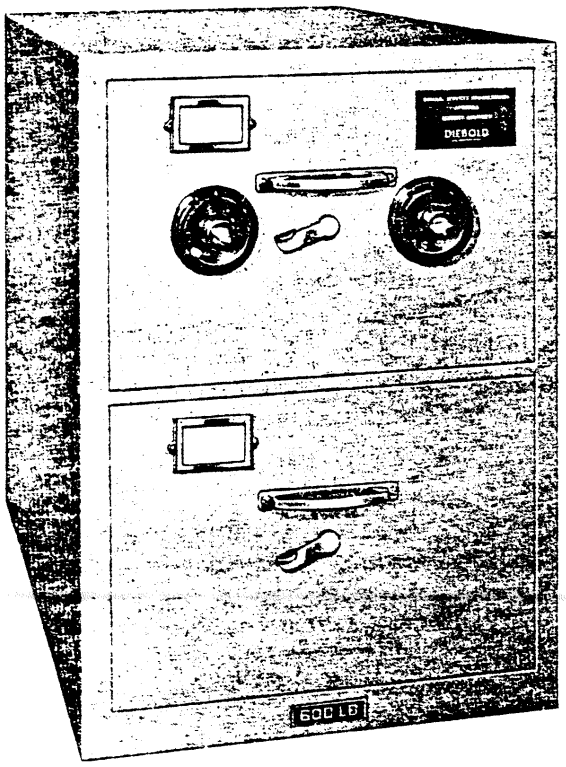


FIGURE 9-2. DISINTEGRATORS/PULVERIZERS



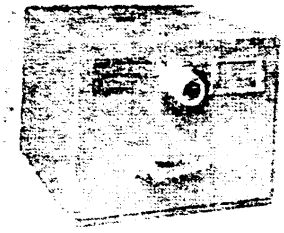


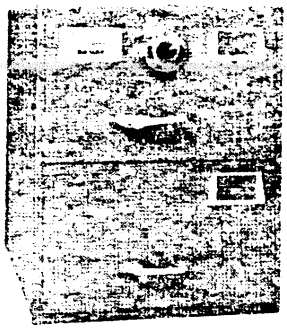
CLASS 6



CLASS 2 CABINET — INSULATED

Letter size only
4 holes
in bottom
for anchoring





CLASS 6

FIGURE 10-2. SECURITY CABINETS

b. The following are descriptions of security filing cabinets that are available on the Federal Supply Schedule for the storage of classified material (see Figure 10-2 for illustrations):

(1) Class 1

The Class 1 security filing cabinet is the only insulated cabinet available on the Federal Supply Schedule. It is available in a 2 drawer or 4 drawer cabinet with one or two locks on the 2 drawer model. The protection provided is expressed on the test certification label as:

30 man-minutes against surreptitious entry
10 man-minutes against forced entry
20 man-hours against lock manipulation
20 man-hours against radiological attack
1 man-hour against fire damage to contents

(2) Class 5

(a) The Class 5 security filing cabinet offers the maximum protection available.

(b) The protection provided is expressed on the test certification label as:

30 man-minutes against surreptitious entry
10 man-minutes against forced entry
20 man-hours against manipulation of the lock
20 man-hours against radiological attack

(c) Except for the map and plan cabinet, there are currently no Class 5 filing cabinets on the GSA Federal Supply Schedule; however, several firms have submitted bids to GSA for approval.

(d) Before a decision is made to purchase a Class 5 cabinet, the additional security provided by the 10 man-minute forced entry feature must be balanced against the extra cost involved.

(3) Class 6

(a) The Class 6 security filing cabinet affords the same protection as the Class 5 except that there is no certified

forced entry protection. It is available in 2, 4 and 5 drawer cabinets and in a map and plan cabinet. The protection provided is expressed on the test certification label as:

30 man-minutes against surreptitious entry
20 man-hours against manipulation of the lock
20 man-hours against radiological attack
No forced entry test requirement

(b) Key-change combination locks should be specified when ordering.

10-5 SECURITY DESK. Office furniture items allow fabrication of a 2-drawer or 4-drawer desk, or an L-unit arrangement by using Class 6 standard 2-drawer containers as pedestals (Figure 10-3). Desk top units, support panels, and necessary hardware are listed under Class 7110, Steel Unitized Office Furniture, Federal Supply Service Stores Stock Catalog.

10-6 MAP AND PLAN SECURITY CABINET. The Mosler Safe Co. manufactures the Map and Plan Security Cabinet in both Class 5 and Class 6 models. The Schwab Safe Company, Inc., manufactures this type of security cabinet only in the Class 5 model (Figure 10-3). NOTE: Both the Map and Plan security cabinets and the Weapons storage container (Par. 10-8) can be equipped with individually locked compartments suitable for the protection of funds and other valuables.

10-7 MONEY SAFE. The Mosler Safe Co. manufactures a Class 5 money safe with or without a channel base (Figure 10-3).

10-8 WEAPONS STORAGE CONTAINER. The Mosler Safe Co. manufactures a Class 5 weapons container. Seven drawers is a standard configuration in the container (Figure 10-3).

10-9 VAULTS AND STRONGROOMS.

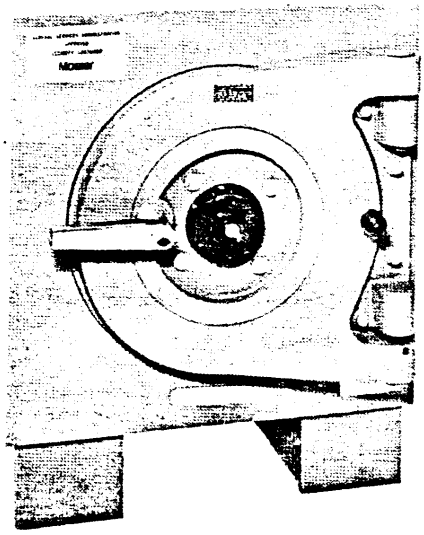
a. Vaults. When new vaults or strongrooms are constructed, they should be built in accordance with the standards specified herein. These criteria and standards give a basis for achieving a uniform character for the construction of security vaults within the Department of Transportation.

(1) Specifications.

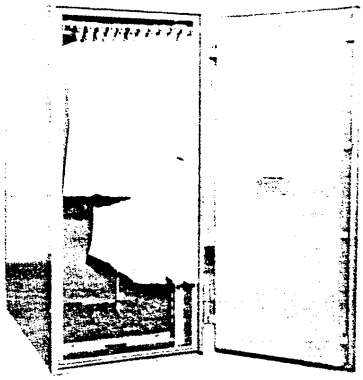
(a) Class A:

(i) Floor and Walls. Eight-inch-thick reinforced concrete. Walls to extend to the underside of the roof slab above.

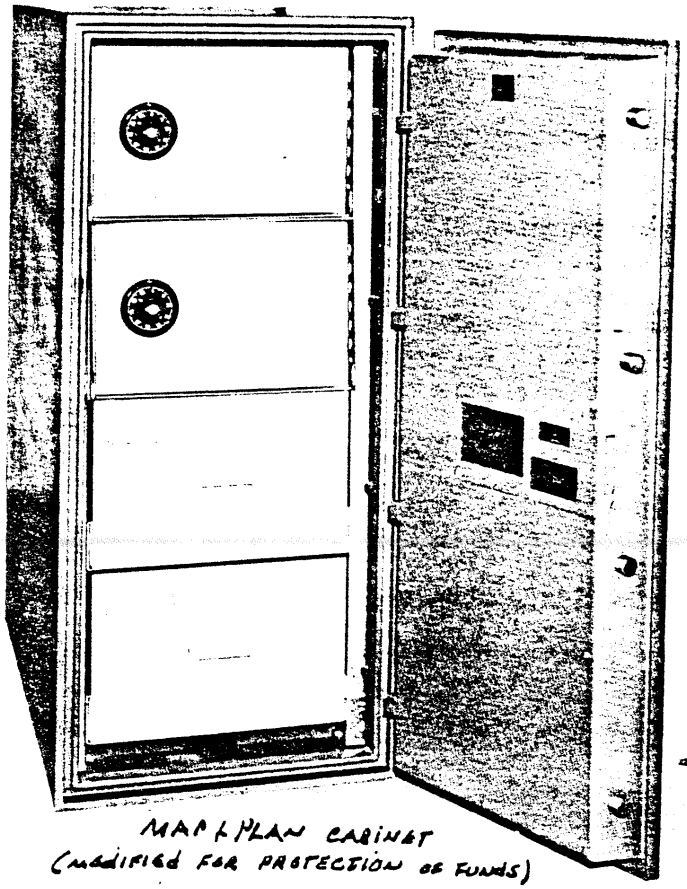
MAP & PLAN (Modified)



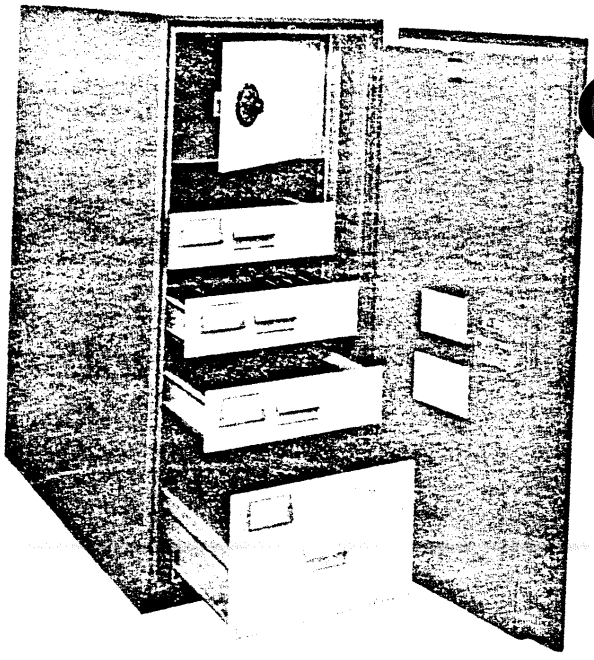
MONEY SAFE



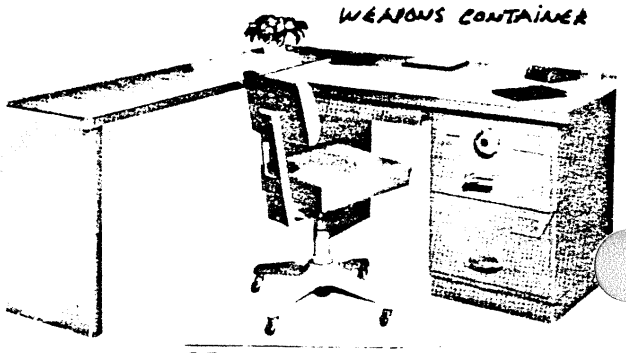
MAP & PLAN



MAP & PLAN CABINET
(Modified for Protection of Funds)



WEAPONS CONTAINER



SECURITY DESK

FIGURE 10-3 SPECIAL CONTAINERS

(ii) Roof. Monolithic reinforced-concrete slab of a thickness to be determined by structural requirements, but not less thick than the walls and floors.

(iii) Ceiling. Where the roof construction is not in accordance with paragraph (ii) above, a normal reinforced-concrete slab will be placed over the vault area at a height not to exceed 9 feet.

(iv) Vault Door and Frame Unit. The vault door and frame shall conform to Federal specifications for Class 5 vault doors (Figure 10-4).

(b) Class B:

(i) Floor. Monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches thick.

(ii) Walls. Not less than 8-inch-thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used, and shall be in seismic areas.

(iii) Roof. Monolithic reinforced-concrete slab of a thickness to be determined by structural requirements, but not less than 4 inches thick.

(iv) Ceiling. Where the roof construction is not in accordance with paragraph (iii) above, a normal reinforced-concrete slab will be placed over the vault at a height not to exceed 9 feet.

(c) Class C:

(i) Floor. See paragraph b(i).

(ii) Walls. Not less than 8-inch-thick hollow clay tile vertical cell (double shell) or concrete block (thick shell). Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used, and shall be used in seismic areas. Walls back of the exterior wall-faction of the building shall be concrete solid masonry, or hollow masonry filled with concrete and steel reinforced bars.

(iii) Roof. See paragraph b(iii).

(iv) Ceiling. See paragraph b(iv).

(v) Vault Door and Frame Unit. The vault door and frame unit shall conform to Federal specifications for Class 6 vault doors.

(2) Safety and Emergency Devices.

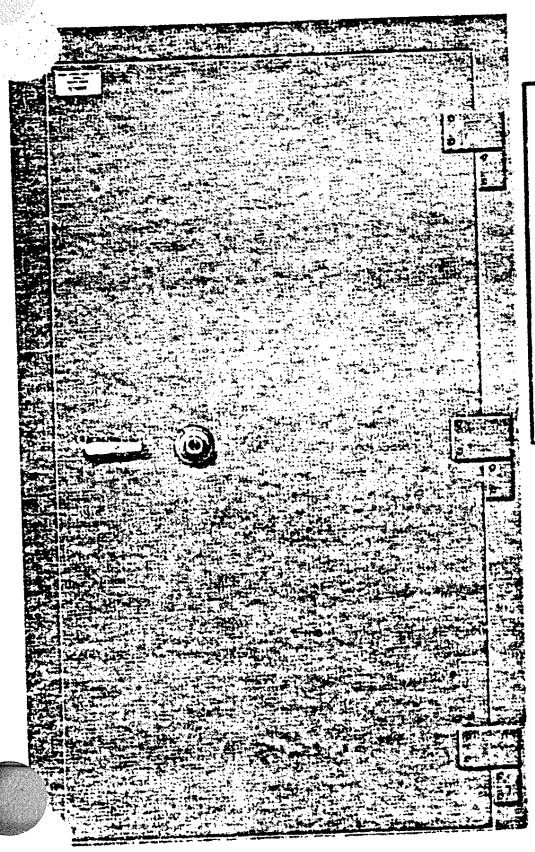
(a) The vault door shall be equipped with an emergency escape and relocking device (Figure 10-4). The escape device, not activated by the exterior locking device, shall be accessible on the inside only and shall be permanently attached to the inside of the door to permit escape by persons inside the vault. The device shall be designed and installed so that drilling and rapping of the door from the outside will not give access to the vault by actuating the escape device. Vault doors conforming to Federal specifications will meet this requirement.

(b) A decal containing emergency operating instructions shall be permanently affixed on the inside of the door. Each vault shall be equipped with an interior alarm switch or device (such as a telephone, radio, or intercom) to permit a person in a vault to communicate with the vault custodian, guard, or guard post so as to obtain his release. Further, the vault shall be equipped with a luminous-type light switch and, if the vault is otherwise unlighted, an emergency light shall be provided.

(3) Structural design. In addition to the requirements given above, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described above, the concrete shall be poured in place, and will have a minimum 28-day compressive strength of 2,500 psi.

b. Approved Security Vault Doors.

(1) Security vault doors are manufactured by the Mosler Safe Co., Hamilton, Ohio, and by Diebold, Inc., Canton, Ohio, in Classes 5 and 6, respectively. As in the case of security filing cabinets, before a decision is made to purchase a Class 5 vault door, the 10 man-minute forced entry feature, not found in the Class 6 vault door, must be compared with the cost differential between the two



PROTECTION

This is a U.S. Government Class 5 Vault Door which has been tested and approved by the Government under Fed. Spec. AA-D-600B. It affords the following security protection:

30 MAN-MINUTES AGAINST SURREPTITIOUS ENTRY.
10 MAN-MINUTES AGAINST FORCED ENTRY.
20 MAN-HOURS AGAINST MANIPULATION OF THE LOCK.
20 MAN-HOURS AGAINST RADIOLOGICAL ATTACK.

The protection certified above applies only to the door and not to the vault proper.

Federal Specification AA-D-600B

Escape Device...

An escape device is attached on the inside face of the door to permit escape for persons locked inside the vault.

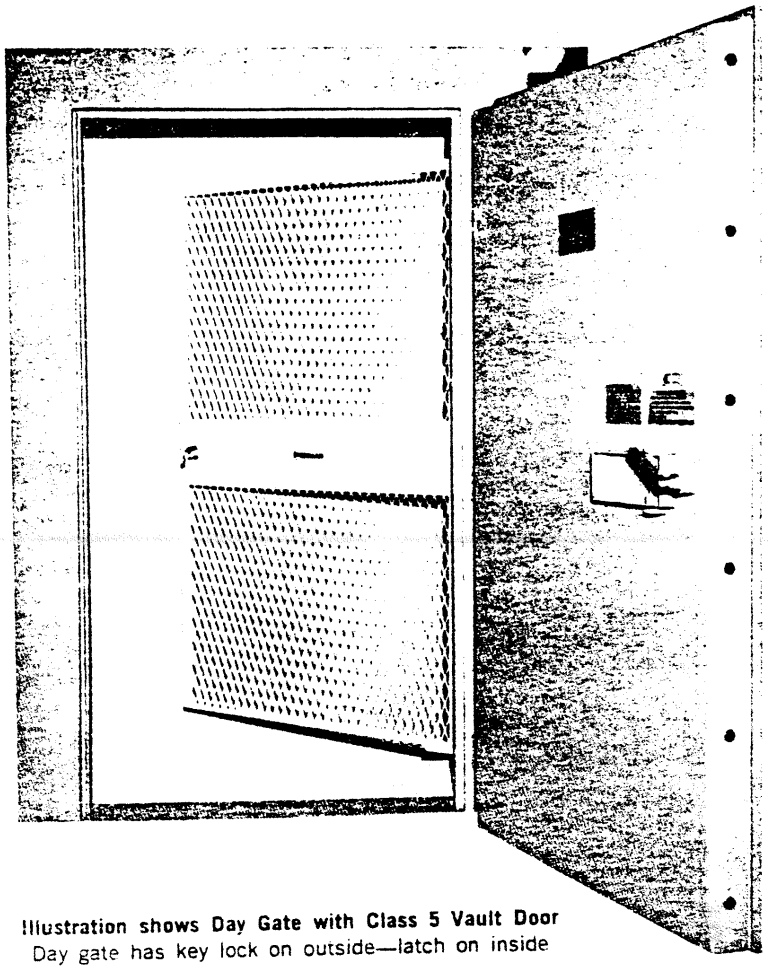


Illustration shows Day Gate with Class 5 Vault Door
Day gate has key lock on outside—latch on inside

FIGURE 10-4. CLASS 5 VAULT DOOR

classes. Additionally, the expense involved in the construction of a Class A vault, requiring a Class 5 door, is considerably greater than that found in erecting a Class C vault with a Class 6 vault door.

(2) The Mosler Safe Co. Class 5 vault door has the following features:

(a) An escape device mounted on the inside face of the door to permit the exit of persons who may become locked inside the vault.

(b) Optional right or left swing door.

(c) Optional day-gate which is designed to be used as a personnel access control measure while the vault area is occupied.

(d) An optional optical device known as a "peep sight." This is a wide-angle tubular optical device approximately 60 inches from the vault floor which provides observation from inside or, if desired, from outside the vault.

(e) Adjustable wall flanges that accommodate 6-, 7-, 8-, 9-, 10-, 11-, 12-, or 14-inch walls and that provide for + or - ½-inch variation.

(f) A key- or hand-change type combination lock.

(3) The Diebold class 6 vault door is different from the Mosler door as follows:

(a) Adjustable wall flanges accommodate only 6-, 8-, 10-, and 12-inch walls.

(b) Only a key-change type combination is available.

(4) Procurement of security vault doors is subject to the Government maximum order limitation of $25,000 and any desired options should be specified when placing orders. Additionally, the finished thickness of the vault walls must be specified in order that proper adjustable wall flanges may be provided.

c. Strongrooms. A strongroom should be considered an interior space enclosed by, or separated from, other similar spaces by four walls, a ceiling, and a floor, all of which are normally constructed of solid building materials. Under this criteria, rooms having false ceilings and walls constructed of fabrics or other similar material shall not qualify as a strongroom. Specific construction standards are as follows:

(1) Hardware. Heavy-duty builder's hardware shall be used in construction, and all screws, nuts, bolts, hasps, clamps, bars, hinges, pins, etc., shall be securely fastened to preclude surreptitious entry and assure visual evidence of forced entry. Hardware accessible from outside the area shall be peened, brazed, or spot welded to preclude removal.

(2) Walls and ceilings. Construction shall be of plaster, gypsum board, metal, hardboard, wood, plywood, No. 9 gauge, 2-inch wire mesh or stronger, or other materials offering similar resistance to, or evidence of, unauthorized entry into the area. Insert type panels shall not be used.

(3) Floors. Floors shall be of solid construction, utilizing materials such as concrete, ceramic tile, wood, etc.

(4) Windows. Window openings shall be fitted with ½-inch bars (separated by no more than 6 inches), plus cross bars to prevent spreading or No. 9 gauge mesh fastened by bolts extending through the wall and secured on the inside of the window board. In addition to being kept closed at all times, the windows shall also be opaqued by any practical method, such as paint on both sides of the window, tempered masonite, sheet metal, cement-asbestos board, etc.

(5) Miscellaneous openings. Where ducts, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, they shall be equipped with man-safe barriers such as wire mesh (No. 9 gauge, 2-inch-square mesh) or steel bars of at least ½-inch in diameter extending across their width with a maximum space of 6 inches between the bars. The steel bars shall be securely fastened at both ends to preclude removal, with cross bars to prevent spreading. Where wire mesh or steel bars are used, care shall be exercised to insure that classified material within the room cannot be removed or viewed with the aid of any type of instrument. Door traps shall be dead-bolted inside the room.

(6) Doors. Doors may be of metal construction or solid wood reinforced with a metal panel on the inside. When doors are used in pairs, an astragal (overlapping molding) will be used where the doors meet. When the construction is of No. 9 gauge, 2-inch wire mesh, a door constructed of similar material may also be used. However, the wire mesh door shall be reinforced with a metal panel at least 36 inches wide from floor to ceiling welded to the inside of the wire mesh wall next to the locking device.

(7) Door Louvers and Baffle Plates. When used, they shall be reinforced with wire mesh (No. 9 gauge, 2-inch-square mesh) fastened to the inside of the door.

(8) Door-locking Devices. Doors shall be secured by a built-in three-position, group 1 or group 1R combination lock. When the construction is No. 9 gauge, 2-inch wire mesh, the locking device shall be alarmed to detect attempted tampering with the lock.

10-9 APPROVED COMBINATION LOCKS.

a. Federal specifications under which security filing cabinets and security vault doors are manufactured require that the units be equipped with a changeable combination lock.

(1) Combination locks are available with either hand-change and key-change; however, only the latter should be specified when ordering the container. Changing the combination in a hand-change lock requires the removal of the discs from the lock and changing each disc from the old to the new combination. Changing the combination of a key-change lock simply requires the use of a special change key that is inserted into the lock case, permitting the new combination to be dialed.

(2) Replacement locks may be purchased from the Mosler Safe Co., Hamilton, Ohio, and Sargent & Greenleaf, Inc., Rochester, N.Y., or through their local representatives. In all replacement orders, it is necessary to indicate the style, serial number, and date of manufacture of the filing cabinet for which a replacement is being sought. This information is required so that the correct spindle length can be provided. Figure 10-5 shows the types of security combination locks available for separate purchase and their approximate cost.

b. Combination Padlocks.

(1) The primary use of the combination padlock within the Department of Transportation is on the lockbar type filing cabinet. For many years the only combination lock designated as a security padlock and available through the Federal Supply Schedule was the Sargent & Greenleaf Model 8088 (Figure 10-5). This padlock did not meet the Federal specifications and was accepted on the schedule only in order to have a padlock available.

(2) Sargent & Greenleaf, Inc., now manufactures two high-security type combination padlocks (Figure 10-5) that do meet Federal specifications and that are available through the Federal Supply Schedule. The stated protection afforded by the concealed-shackle model 8065 is:

30 man-minutes against manipulation of the lock
30 man-minutes against radiological attack
15 man-minutes against surreptitious entry

The unique design of Model 8065 with its versatile security cover permits it to be used either as a removable padlock in conjunction with locking bar cabinets and other conventional hasp type applications, or by fastening the security cover to the surface of a unit. It can be applied on desks, storage cabinets, filing cabinets, sliding door cabinets and virtually any type of container through use of an eyelet or loop designed to suit the tolerances of the opening in the rear of the padlock.

(3) The stated protection afforded by the exposed shackle model 8077 is:

30 man-minutes against manipulation of the lock
30 man-minutes against radiological attack
10 man-minutes against surreptitious entry

c. Proper Use of Combination Locks.

(1) To ensure effectiveness of combination locks, the following procedures should be observed:

(a) Combinations should be known only to those persons whose official duties require access to the container.

(b) The combination should be changed at the time received, at the time any person having a knowledge of it leaves the organizational unit, at any time there is reason to believe it has been compromised, or in any case every 12 months.

(c) The written combination to a lock should be of the same classification as the material in the container.

(d) Combination records should be sealed in an envelope and kept on file by the security office.

(e) In selecting combination numbers, multiples of 5, simple ascending or descending arithmetical series, and personal data such as birthdates and serial numbers should be avoided.

(f) If setting a combination, numbers that are widely separated shall be used. This can be achieved by dividing the dial into three parts and using a number from each third as one of the combination numbers.

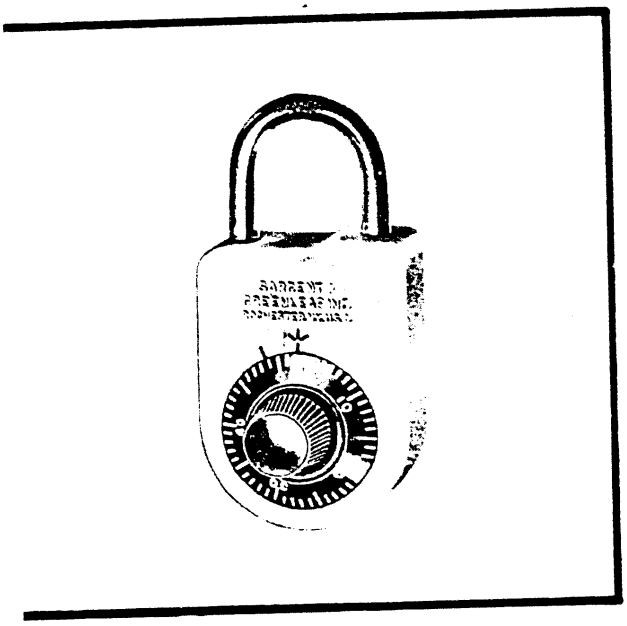
(g) The same combination will not be used for more than one container in any one component.

(h) To prevent a lockout, a new combination should be tried at least twice before closing the container.

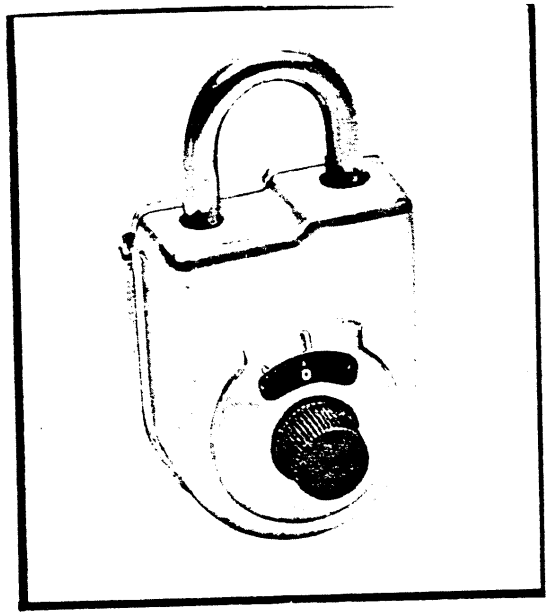
(i) The dial should be turned four or more complete revolutions in the same direction when securing containers.

Manufacturer	Model description	Order	Approximate cost
Sargent & Greenleaf ...	T8430 XD28X	1-9	$28.13
		10-99	27.02
		100-499	26.05
Master	No. 76010 (hand change)		27.45
	No. 76013 (key change)		30.05

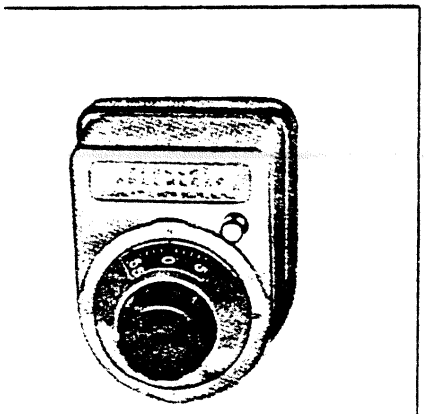
Available Security Combination Locks.



8088 PADLOCK



8077 PADLOCK



Model 8065 Concealed Shackle.

FIGURE 10-5. COMBINATION PADLOCKS

CHAPTER XI

11-1 SECURITY SURVEYS AND INSPECTIONS. Security surveys and inspections are vital to the conduct of any security program, whether it involves the protection of Government assets, information or personnel. To draw a distinction, a survey is usually thought of in terms of determining what needs to be done in order to provide adequate protection at a facility, while an inspection is conducted primarily to determine whether or not the existing controls are adequate and if they are being enforced. Each is an indispensable element in any security operation.

11-2 SURVEYS. There are four basic types of surveys.

a. Initial Survey. This is the first survey at a facility. This is when the decisions have to be made as to what security controls are needed, how they should be implemented, by whom and when. What is done at this point will set the stage for the future security of the facility. For this reason the survey must be both thorough and precise concerning the type of security controls that would be appropriate. Personnel conducting the survey should have a complete set of drawings of the facility which depict all areas within the facility, including all access points and any adjacent areas belonging to the facility, such as parking lots, warehouses, etc. The basic criteria against which the facility should be evaluated are:

(1) Relative Criticality. All facilities are, to some degree, valuable to the overall mission of the Department. The difference is only one of degree. In making this assessment, the question should be asked what the effect on DOT (and possibly on National Security) would be as a result of the partial or complete loss of the facility. If it would have a major impact on transportation safety and/or on national security or would jeopardize a vital mission, the criticality factor should be rated high, especially in the absence of any redundancy capability.

(2) Relative Vulnerability. The susceptibility of a facility to damage, theft of property or information, or even destruction, is dependent upon such factors as: the mission of the facility, its size and configuration, its physical location (i.e., high or low crime area), proximity of law enforcement agencies, and the type of property at the facility that would attract the criminal element because it lends itself to easy resale or illegal use; such as, office machines, firearms, drugs, cash or expensive personal possessions. The presence of classified and/or sensitive and proprietary data would also enter into the rating. Any combination of these factors would cause the facility to be rated high on the vulnerability scale.

b. Follow-Up Survey. The purpose of this survey is to determine whether or not the initial recommendations had been carried out and, if not, why not. The fact that work orders may have been issued is no guarantee that the work will be performed in a timely manner. Any indication that the scheduled work is not proceeding on time or has not received the priority it warrants, should be brought to the attention of the management officials at the facility.

c. Supplemental Survey. This type of survey is performed when changes occur in the organization, mission or physical aspects of the facility that could possibly alter or affect the overall security program.

d. Special Survey. This type is conducted for a specific purpose, such as, creation of a controlled area, extensive damage at the facility due to man-made or natural disasters, a series of thefts at the facility and unforeseen situations.

e. Survey Reports. The cognizant security element should maintain survey reports covering all of the facilities under their cognizance, providing such information as: a physical description of the facility, location, population, basic mission(s), key management officials, the primary security considerations at the facility (e.g., high-value items, classified material, monies, armory) and the basic security plan for protecting the personnel and property. These reports would serve the dual purpose of providing the security element with a readily accessible security status of each facility and for scheduling inspections.

11-3 INSPECTIONS. Once the basic security controls are established, the facility should be placed on an appropriate inspection schedule. The frequency of the inspections will, of course, vary based on the key factors discussed in the preceeding paragraph; namely, the criticality and mission of the facility and/or its relative vulnerability to theft, sabotage and similar incidents. In applying this general criteria to the wide range of facilities within DOT, security elements should assign facilities under their cognizance into the following categories:

a. Category 1. These facilities warrant inspection on an annual basis. They are ones that are highly essential to transportation safety or other vital DOT missions. The fact that a facility is unmanned should not be a reason for automatically excluding it from this category. There are a number of unmanned facilities that perform a vital function far in excess of that performed at many manned facilities. Facilities that produce or possess large volumes of classified material, or which have ADP systems, would also fall into this category, which would be in compliance with the inspection requirements set forth in DOT 1640.4 and 1640.8, respectively.

b. Category 2. These facilities warrant inspection at least every three years. They are not as critical or vulnerable as Category 1 facilities, but are important in terms of transportation safety or other DOT missions. For example, if there is a backup or redundancy capability for the facility's function, then it could be consigned to Category 2 instead of Category 1.

c. Category 3. These facilities are not required to be inspected on a regularly scheduled basis, but rather on an "as needed" basis; for example in the event of a serious security incident or a series of reported thefts or attempted break-ins. They have some security interest, but are not considered vital in terms of criticality or vulnerability. Most of the smaller manned and unmanned facilities would tend to fall into this category.

11-4 CONDUCT OF INSPECTIONS. It would be impractical to develop a rigid set of rules or standard format for conducting inspections. As no two facilities are identical in every aspect, likewise no two inspections are exactly similar. There are, however, some common denominators that apply equally to all inspections. They are:

a. Preparation or Planning Stage. This is an indispensable element in any inspection. Planning helps the inspector avoid doing a haphazard inspection with negligible results. Among the things that should be routinely done during this stage are: reviewing past inspection reports, and becoming acquainted with the facility's security history, organizational structure, its mission, composition of the work force, work hours and the relative importance of the facility. Finally, preparing an informal checklist of the key points to be reviewed during the inspection and in what order.

b. Inspection Stage. Depth of the inspection will depend upon criticality of the facility, recency and findings of prior inspections, indications of possible security problems and similar considerations. The inspection will not only include the planned checklist coverage, but should explore potential security problems surfaced during the inspection. Sufficient sampling and checks will be made to support conclusive findings, either favorable or unfavorable patterns and trends will be looked for rather than isolated deficiencies. Facility security procedures and awareness will be checked. Written inspection notes and supporting material will be prepared. Attachment 5 contains a physical security inspection checklist that could be adapted accordingly.

c. Analysis Stage. Prior to leaving the facility the work notes shall be checked for completeness and accuracy. Significant findings shall be identified, and when appropriate, facility officials will be given a verbal briefing on such findings. Agreements on readily-correctable actions may be made, but will be documented in the inspection report.

d. Reporting Stage. The inspection report is a key step in the inspection process. Inadequate reporting can nullify an otherwise effective inspection. Findings shall be stated concisely and precisely. Appropriate recommendations for correcting deficiencies shall be provided. The report shall request timely response describing corrective actions taken or planned.

e. Follow-Up Stage. This is the stage when it is determined whether or not the necessary corrective action had been taken on the security deficiencies contained in the inspection report. Except for minor deficiencies, a reinspection of the facility should be scheduled within a reasonable time after receiving managements' reply to the report of inspection. The reinspection should be limited in scope and concentrate only on the previously cited deficiencies. As in the case of the inspection report, management should be advised in writing of the results of the follow-up inspection.

11-5 INSPECTION ASSISTANCE. In order to meet the established inspection schedules, the security element should solicit the cooperation of personnel in other non-security functions who have occasion to visit both manned and unmanned facilities. For example: Personnel in the FAA Airway Facilities Division who conduct annual safety inspections at unmanned FAA facilities. If provided with a security checklist by the security element, such personnel could lend valuable assistance by checking on the status of security at the facility with a minimum expenditure of time and effort. Their reports should be submitted to the security element for review and appropriate follow-up action.

CHAPTER XII

12-1 INCIDENT REPORTING. An incident reporting program is an essential element in any security program. It is not enough to develop a comprehensive set of security controls for a facility without being concerned about the loss/theft or malicious damage (including arson) of Government property. One test of how effectively the security controls are working is the number and type of security incidents that occur at a facility.

12-2 REPORTING REQUIREMENTS. The timely reporting of thefts, losses or malicious damage of Government property to the appropriate security element is imperative. The quicker the incident report is made, the greater the possibility of recovering the property and apprehending the perpetrator. In addition to the timeliness of the reports, they must be accurate and complete, especially in the description of the property involved and the circumstances surrounding the incident. What is done with the report after it is received by the security element is also a good measurement of the programs' effectiveness. If the reports are not analyzed or acted upon in a prompt, decisive manner, the reporting system is undermined.

12-3 INDIVIDUAL RESPONSIBILITIES. Under the provisions of DOT 1600.20, an employee discovering the theft or malicious damage or loss of Government property has an obligation to report the incident immediately to the cognizant security element and/or to the Federal Bureau of Investigation or the local law enforcement agency. In the event there is no servicing security element available, a report furnished to the FBI or local agency is sufficient, provided that a follow-up report is sent to the designated headquarters security element in Washington, D.C. (For employees assigned to the DOT Headquarters facilities, the reporting procedures set forth in DOT 1660.2 apply.) It should be noted that the channels for reporting missing or stolen property by property custodians under the property management regulations does not supplant the requirement to report such matters to the security element. However, through local arrangements between the security and property management offices, reporting procedures can be developed that would satisfy both the property control and security requirements.

12-4 RESPONSIBILITIES OF THE SERVICING SECURITY ELEMENT. Upon receiving a report involving the loss/theft or malicious damage of Government property, the servicing security element should:

a. Review it for accuracy and completeness: insuring that it presents a complete picture of what happened, when and where and who or what may have been responsible for the incident.

b. Verify that the FBI and/or the local law enforcement agency had been notified of the incident. The prescribed reporting format should include a space or block indicating whether or not such notification had been given.

c. Initiate, if appropriate, an investigation of the incident, including, if need be, an on-site visit where the incident occurred. This decision should be based on the following:

(1) Is this an isolated incident or one of a series of such incidents which may indicate a possible pattern?

(2) Does the stolen, lost or damaged property have a high-dollar value or importance to the mission of the facility?

(3) Is it the type of stolen property that could be readily converted to personal use or sold illegally; for example, a typewriter versus a specialized piece of test equipment?

(4) Does the description of the circumstances surrounding the incident reveal a possible weakness or loophole in the security controls at the facility? If the facility had not been previously surveyed or inspected, the reported incident could provide the basis for scheduling a visit in the immediate future.

(5) Advise the designated headquarters office by the most expeditious means available if the incident is of such gravity or importance as to warrant alerting the headquarters; for example, the destruction by arson of an entire facility and its contents or the wholesale theft of office equipment from a particular facility. For other than unusual incident reports, security field elements should submit summary reports to their headquarters offices on a regularly scheduled basis, categorizing the security incidents that occurred within the established reporting period.

12-5 REPORTING FORMAT. At GSA leased or managed facilities, the GSA Form 182, Report of Loss or Theft, is the standard reporting form. Copies of the form may be obtained from the GSA Regional Office or the GSA building manager's office. Although not specifically designed for that purpose, it may also be used to report the malicious damage of Government property. At DOT owned facilities, reports may be submitted in the form of a memorandum provided that the same basic information is furnished as required on the GSA Form 182. Follow-up reports should reference the original report, for instance, when an item previously reported as missing is later recovered.

-6 RECORDS. The designated headquarters office within the administrations shall compile and maintain statistical data reflecting the total dollar-value of stolen, lost or maliciously damaged property, including unreconciled personal property uncovered through property inventories and/or the property management reporting system. Such data should be compiled on an annual basis, and be subject to review and analysis by the headquarters security elements.

GSA FEDERAL PROTECTIVE SERVICE REGIONAL OFFICES

REGION 1 (Maine, New Hampshire, Vermont, Massachusetts, Connecticut, Rhode Island).

704 John W. McCormack Post Office and Courthouse
Boston, Massachusetts 02109
(617) 223-5374
Telecopier: 223-5053

REGION 2 (New York, New Jersey, Virgin Islands, Puerto Rico).

26 Federal Plaza, New York, NY 10007
(212) 264-4252
Telecopier: 264-3635

REGION 3 (Pennsylvania, Maryland, Delaware, District of Columbia, Virginia, West Virginia).

Regional Office Building, 7th & D St., S.W., Washington, D.C.
(202) 962-8587
Telecopier: 963-5131

REGION 4 (North Carolina, South Carolina, Georgia, Florida, Kentucky, Tennessee, Alabama, Mississippi).

1776 Peachtree St., N.W., Atlanta, Georgia 30309
(404) 526-3356
Telecopier: 526-3356 or 526-3360

REGION 5 (Ohio, Indiana, Illinois, Wisconsin, Michigan, Minnesota).

Everett McKinley Dirksen Bldg., 230 S. Dearborn St., 36th Floor
Chicago, Illinois 60604
(312) 353-1496
Telecopier: 353-1858

REGION 6 (Missouri, Iowa, Nebraska, Kansas).

Federal Office Building, 1500 East Bannister Rd.,
Kansas City, Missouri 64131
(816) 926-7025
Telecopier: 926-7233

REGION 7 (Arkansas, Louisiana, New Mexico, Oklahoma, Texas).

Federal Office Building, 819 Taylor St., Fort Worth, Texas 76102
(817) 334-3557
Control Center: 334-2888
Telecopier: 334-2525

REGION 8 (Colorado, Montana, Utah, Wyoming).

Building 41, Denver Federal Center, Denver, Colorado 80225
(303) 234-3641
Telecopier: 234-2968

REGION 9 (Arizona, California, Guam, Hawaii, Nevada).

525 Market Street, San Francisco, California 94105
(415) 556-1421
Telecopier: 556-3377

REGION 10 (Alaska, Idaho, Oregon, Washington).

GSA Center, Auburn, Washington 98002
(206) 833-5509
Telecopier: 833-5530

BOMB THREAT QUESTIONNAIRE

2-182a (2-9-76)

FBI BOMB DATA PROGRAM

PLACE THIS CARD UNDER YOUR TELEPHONE

QUESTIONS TO ASK:

1. When is bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

EXACT WORDING OF THE THREAT:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Sex of caller: _____ Race: _____

Age: _____ Length of call: _____

Number at which call is received:

_____

Time: _____ Date: _ _ _

FBI DOT

BOMB THREAT

CALLER'S VOICE:

___ Calm	___ Nasal
___ Angry	___ Stutter
___ Excited	___ Lisp
___ Slow	___ Raspy
___ Rapid	___ Deep
___ Soft	___ Ragged
___ Loud	___ Clearing throat
___ Laughter	___ Deep breathing
___ Crying	___ Cracking voice
___ Normal	___ Disguised
___ Distinct	___ Accent
___ Slurred	___ Familiar

If voice is familiar, who did it sound like?

_____

_____

BACKGROUND SOUNDS:

___ Street noises	___ Factory machinery
___ Crockery	___ Animal noises
___ Voices	___ Clear
___ PA System	___ Static
___ Music	___ Local
___ House noises	___ Long distance
___ Motor	___ Booth
___ Office machinery	Other _____
	_____
	_____

THREAT LANGUAGE:

___ Well spoken (educated)	___ Incoherent
___ Foul	___ Taped
___ Irrational	___ Message read by threat maker

REMARKS: _____

_____

_____

_____

Report call immediately to:

_____ .

Phone number _____ .

Date _ _ _ .

Name _____ .

Position _____ .

Phone number _____ .

ILLUMINATION STANDARDS

DEFINITIONS

a. Foot-Candles. One foot-candle is the amount of light falling on a surface one foot from the light source of one candle power. This measurement is made at the surface being illuminated with an illumination meter calibrated in foot candles. A light source of a given candle power rating will produce the same foot candle rating only on surfaces equidistant from the light source. Since the quality of light received at a surface varies inversely as the square of the distance between the source and the surface, the foot-candles will decrease as distance is increased.

b. Horizontal Illumination. Horizontal illumination is the illumination expressed in foot candles on a horizontal surface. The surface is considered at ground level.

c. Vertical Illumination. Vertical illumination is the illumination expressed in foot-candles on a vertical surface.

SPECIFICATIONS

Ways and means of implementing the below listed specifications are contained in the American National Standards Institute Inc. Practices, "Protective Lighting RP-10" June 1970, prepared under the sponsorship of the Illuminating Engineering Society and published by the American National Standards Institute Inc, 29 West 39th Street, New York, New York. Copies may be obtained by writing Publications Department, Illuminating Engineering Society, 345 East 47th Street, New York, New York 10017.

The illumination of boundaries, entrances, structures and areas shall be in accordance with the following standards: (Foot candles refer to the minimum horizontal illumination at ground level except where otherwise stated.)

a. Isolated Fence Boundaries. Where the approach area is clear of obstruction for 100 to 300 feet outside the fence and inside structures are 100 feet or more from the fence and where intentional outward glare is not objectionable, lighting shall be provided as follows:

(1) Width of lighted strip - 210 feet divided into two zones:

Zone I - From 10 feet inside to 25 feet outside the boundary (fence).

Zone II - From 25 feet outside to 200 feet outside the boundary (glare projection).

(2) Minimum Illumination within lighted strip: 0.15 foot candle at any point measured on a vertical plane 3 feet above ground and parallel to the boundary. In addition, for Zone I, sufficient illumination to assure ready detection of personnel shall be provided as deemed necessary.

b. Semi-Isolated Fenced Boundaries. Where the approach area is clear of obstruction for 60 to 100 feet outside the fence, lighting shall be provided as follows:

(1) Width of lighted strip: 80 feet extending from 10 feet inside to 70 feet outside the boundary.

(2) Minimum illumination within lighted strip: 0.04 foot candle at any point.

c. Non-Isolated Fenced Boundaries. Where the property to be protected is immediately adjacent to operating areas of other activites, civil plants, public thoroughfares, etc., lighting shall be provided as follows:

(1) Width of lighted strip: 60 feet extending from 20 to 30 feet inside to 40 or 30 feet, respectively, outside the boundary.

(2) Minimum illumination within lighted strip: 0.08 foot candle if 40 feet and 0.10 foot candle if 30 feet outside the boundary at any point.

d. Building Face Boundaries. Where faces of buildings are on or within 20 feet of the property line and the public may approach the buildings, lighting shall be provided as follows:

(1) Width of lighted strip: 50 feet extending from building face.

(2) Minimum illumination within lighted strip: 0.10 foot candle at any point.

e. Unfenced Boundaries. Where the property lines are more than 20 feet from buildings and there is no fencing or outdoor operating areas between buildings and property lines, lighting shall be provided as follows:

(1) Width of lighted strip: 80 feet outward from the building in the unobstructed area.

(2) Minimum illumination within lighted strip: 0.04 foot candle at any point.

f. Waterfront Boundaries. Where fenced or unfenced property lines are at or adjacent to bodies of water, lighting shall be provided as follows, except that navigable water less than 15 feet in width shall be classed under a. to e. above as though the body of water were not present: (Caution: Coast Guard officials shall be consulted for approval of proposed protective lighting adjacent to navigable waters.)

(1) Width of lighted strip: 60 feet extending from 10 feet inside to 50 feet outside the boundary.

(2) Minimum illumination within lighted strip: 0.10 foot candle at any point.

g. Entrances. At gates, doors, or passages authorized for constant or occasional use at night, luminaries shall be so located as to facilitate recognition of persons, examination of credentials and inspection of vehicles, and the lighting shall be provided as follows:

(1) Extent of lighted area: Width of road or walkway extending 25 feet inside and outside boundary gate for pedestrian entrances, and width of road extending 50 feet inside and outside boundary gate for vehicular entrances.

(2) Minimum illumination within lighted area: 2.0 foot candles (pedestrian) or 1.0 foot candle (vehicular) at any point.

h. Industrial Thoroughfares within Security Areas. Industrial thoroughfares within security areas shall be provided with the following minimum illumination:

(1) 0.05 foot candle at any point when not bordered by buildings.

(2) 0.20 foot candle at any point when bordered by buildings on one or both sides.

31 JUL 1980

i. Open Yards and Outdoor Spaces. (Material storage areas, railroad sidings, truck parking areas, etc.) Within security areas, the following minimum illumination shall be provided:

(1) Open yards: 0.02 foot candles at any point.

(2) Outdoor storage spaces: 0.10 foot candles at any point.

j. Piers and Docks. Piers and docks included within a security area shall be provided with the following minimum illumination of both water and land approaches (subject to Coast Guard approval):

(1) Land approaches (a. through i. above, as applicable).

(2) Water approaches (entending to a distance of 100 feet from pier): 0.10 foot candles horizontal out to 50 feet and 0.05 foot candles vertical from 50 to 100 feet.

(3) Decks of open piers: 0.10 foot candles.

(4) Underneath piers (when pier construction makes applicable): 0.04 foot candles.

k. Critical Structures. Critical structures most easily and seriously harmed at close range shall be lighted to an intensity of not less than 2.0 foot candles at any point and their vertical surfaces to a height of 8 feet and in the approach area immediately surrounding such structures. Critical structures easily harmed from a distance shall not be specifically lighted, thereby lessening their visibility to persons outside the area.

APPLICATION OF SPECIFICATIONS

Ways and means of implementing the foregoing specifications are contained in the American Standards Practices, "Protective Lighting", prepared under the sponsorship of the Illuminating Engineering Society and published by the American Standards Association, 29 West 39th Street, New York, New York.

TYPES OF PROTECTIVE LIGHTING

Continuous. The most common protective lighting system consists of a series of fixed lights arranged to flood a given area with light continuously during the hours of darkness.

Standby. The standby system of lighting is similar to the continuous lighting system. However, the system is activated either manually or automatically when suspicious activity is detected by guards or an alarm system.

Searchlights.

a. Portable (on the ground). Manually operated, portable searchlights (on carriages or wheels) may be employed to supplement either system

b. Fixed and Semifixed on Towers. When the critical nature of the installation requires use of elevated sentry towers over the perimeter barrier, searchlights that have a 360 degree area of train, and sufficient elevation and depression to permit exploration of suspicious actions in the vicinity of the barrier or in adjacent unlighted areas, should be mounted on the

EMERGENCY POWER

In general, any security area provided with protective lighting should have an emergency power source located within that security area. The emergency power source should be adequate to sustain all security requirements and any other essential service required within the security area. Provisions should be made to insure the immediate availability of the emergency power in the event of the failure of the primary source. Security force personnel should be capable of starting emergency power equipment. If lack of technical knowledge prevents this, plans must provide for responsible personnel to respond immediately to start the equipment. In addition, battery powered lights and essential communications should be available at all times at key locations within the security area in the event of a complete failure of both the primary and emergency sources of power.

TECHNICAL ASPECTS

a. General. The differences in building arrangements, terrain, atmospheric conditions, and other factors necessitate the designing of each protective lighting system to meet the conditions peculiar to each activity or facility.

b. Design. For maximum economy, protective illumination should be curtailed to the barest practicable minimum consistent with the requirements of security. In designing a lighting system, consideration should be given to the local conditions at the installation or activity.

c. Wiring System. Multiple circuits may be used to advantage in protective lighting systems. The circuits should be so arranged that the failure of any one lamp will not darken a long section of a critical or vulnerable area. The protection lighting system should be independent of the activity's lighting system and should be so protected that fires will not interrupt the entire system.

MAINTENANCE

The protective lighting system should provide for simplicity and economy in maintenance and should require only a minimum of shutdown time, routine repairs, cleansing, and replacement.

PROTECTION - CONTROLS AND SWITCHES

Controls and switches for protective lighting systems should be locked, guarded, or both at all times. The most effective means is to have them located in a key guard station or central station similar to the system used in intrusion alarm central station installations.

STANDARDS FOR SHIPBOARD ARMS AND AMMUNITION AREAS

1. Remove any existing expanded metal bulkheads and doors or any light metal bulkheads in ships armory and small arms magazines that don't conform to the minimum standards listed below.

a. Periphery bulkheads shall be minimum of 14 gage sheet steel.

b. Bulkheads constructed of double walled extruded aluminum and aluminum honeycomb shall be replaced with minimum 14 gage sheet steel. Existing aluminum plate bulkheads 1/8 of an inch or thicker may be retained.

c. All welded construction is preferred; however, solid core steel rivets or mechnical fasterners, Mil-Spec Mil-P-23469 or Mil-B-23470 may be used. Rivets must be 1/4 inch diameter minimum. The use of pop rivets is prohibited.

d. Pins for door hinges shall be peened over to prevent removal. In addition, to prevent removal of door in the event the hinge pins are forcibly removed, three (3) "L" shapped security brackets shall be fitted on the inside of the door as shown on enclosure (1). The brackets shall be edge welded to the door stiffeners on the hinged side and extend past the door frame when the door is closed. This is not required if the hinges are located within the space.

e. Door hasps shall be the high security type Mil-H-43905A style 8 or 9 type 304 stainless steel. Welding is the preferred method of fastening hasps to bulkhead and door; however, rivets or mechanical fasteners as per paragraph C.1.c may be used.

f. The access door shall be secured with one high security padlock, Mil-P-24498 type II with a carbide reinforced shackle (NSN 5340-00-799-8016 open shackle) or (NSN 5340-00-799-8248 anti-wedge). These are the only approved padlocks.

g. In lieu of the hasps and padlock above, where possible the HMR Security Products Corporation Tufloc Model 60 series integral hasp and lock should be used. (4 1/2" X 3 1/2" 5340-00-144-7310), (6 7/16" X 3 1/2"/RH-5340-00-144-7311), (6 7/16" X 3 1/2"/LH-5340-00-145-0293), (8 3/8" X 3 1/2" 5340-00-144-7359). See enclosures (10) and (11) for details.

2. All small arms are to be stowed in lockers located in the armory. For units without an armory the locker shall be located in the commanding officer/officer in charge stateroom or the wardroom. The locker shall be constructed as follows:

a. Lockers must be constructed of not less than 14 gage steel sheet (Grade M).

b. Modify locker hinge supports in accordance with enclosure (2).

c. Hasps shall be in accordance with Mil Spec Mil-H-43905A type 304 stainless steel and a high security padlock as per paragraph

SMALL ARMS SECURITY

C.1.f shall be used.

d. In lieu of the hasp and padlock as stated a BMR Security Products Corporation Tufloc, Model 60 integral hasp and lock may be used where possible.

3. For topside ordnance lockers the existing welded, watertight lockers shall be used with high security hardware as specified below.

a. All lockers are to be secured with a high security padlock as per paragraph C.1.f. and hasps, as per enclosures (3) thru (7).

b. The addition of retaining brackets to prevent opening of the locker if the hinges are removed is also required. Enclosures (8) and (9) provide details of the retaining brackets.

c. All hasps and hardware shall be welded.

d. Welding is the preferred method of securing lockers to the ships structure; however, rivets or mechanical fasteners as per paragraph C.1.c may be used.

SECURITY BRACKET

NOTES-

1. MATERIAL: 10.2# P (¼" THK) MILD STEEL.
2. THREE BRACKETS PER DOOR, ONE BEHIND EACH HINGE.
3. IF PANEL STIFFENERS ARE SAME DEPTH AS RIM STIFFENERS CUT BRACKETS ON DOTTED LINE.

CHAPTER III

3-1 PERIMETER CONTROLS. Perimeter protection is the first line of defense in providing physical security for a faciltiy (Figure 3-1). Protecting the outer perimeter of a facility may be accomplished by installing fences or other physical barriers, outside lighting, intrusion detectors or by a patrol force. Often a combination of two or more of these controls will be the most effective.

3-2 PURPOSE OF PERIMETER BARRIERS. In addition to defining the physical limits of a facility and restricting access, a perimeter barrier also:

a. Creates a physical and psychological deterrent to accidental entry.

b. Deters unauthorized entry.

c. Delays intrusion into an area, making the possibility of detection and apprehension more likely.

d. Serves as an effective aid to the guards in controlling access.

e. Facilitates the effective utilization of security forces.

f. Assists in directing the flow of persons and vehicles through designated entrances.

3-3 TYPES OF PHYSICAL BARRIERS. Physical barriers are of two general types -- natural and structural. Natural barriers include mountains, cliffs,

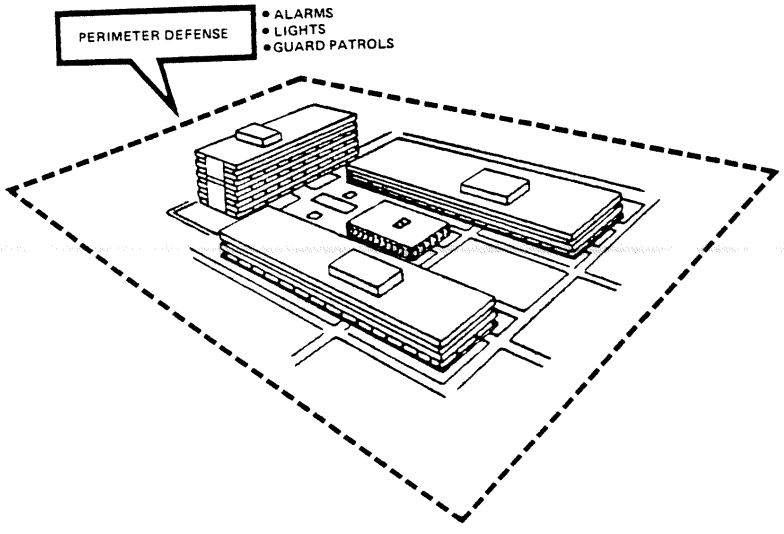


Figure 3.1 – PERIMETER DEFENSE

rivers, etc. Structural barriers are manmade devices such as fences, walls, buildings, grills, bars, or other barriers which deter penetration. To be fully effective, barriers must be under the surveillance of guards. Structural barriers should be considered to supplement natural barriers, if necessary. Structure barriers often imply that chain link fencing is the only acceptable material for this use. A barrier does not need to be constructed of wire fencing to be effective as a security control. In areas where fencing could be utilized, and the appearance of the facility is a factor, proper planning and design can result in an attractive wall or barrier. Such a barrier, if properly designed, can have the same effect as wire fencing without detracting from the appearance of the facility.

3-4 TYPES OF FENCING. The two types of fencing normally used are chain link or barbed wire. The choice is dependent primarily upon the degree of permanence of the facility, availability of materials and construction time. Generally, chain link fencing should be straight to permit unhampered observation and when property lines and location of buildings permit, should be not less than 50 feet from the object of protection.

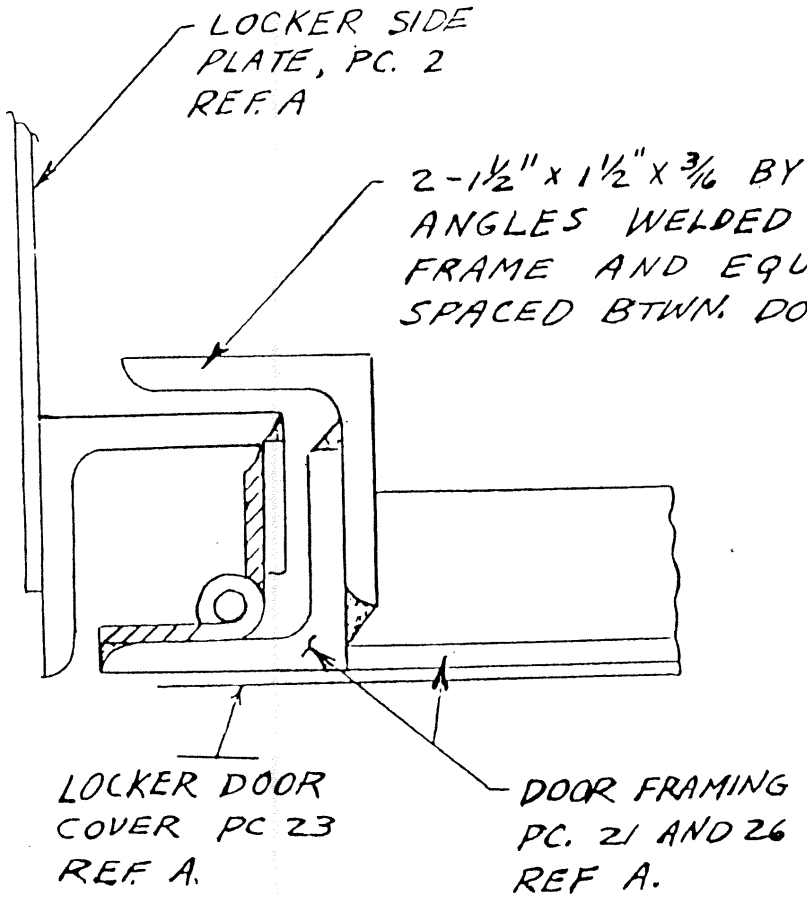
a. Chain Link. Chain link fence, including gates, should be of No. 11 gauge or heavier wire, not less than seven feet in height plus a top guard and with mesh openings not larger than two inches per side with a twisted and barbed selvage at top and bottom (Figure 3-2). It shou be taut and securely fastened to rigid metal posts set in concrete. It should reach within two inches of hard ground or paving, and on sof ground should reach below the surface sufficiently to compensate for shifting soil or sand. Anti-erosion measures such as the use of surface priming may be necessary. Where it traverses culverts, troughs, or other openings larger than 96 square inches in area, the openings must be protected by fencing, iron grills, or other barriers to prevent passage of intruders without impeding drainage. Chain link fencing is low in maintenance costs, is a minimal safety hazard, and yet has openings small enough to prevent the passing of pilfered articles.

b. Barbed Wire. Standard barbed wire is twisted, double strand, No. 12 gauge-wire, with four-point barbs spaced four inches apart. Barbed wire fencing, including gates intended to prevent trespassing, should be not less than seven feet in height plus a top guard, tightly stretched, and firmly affixed to posts not more than six feet apart. Distances between strands should not exceed six inches.

3-5 TOP GUARD. A top guard is an overhang of barbed wire along the top of a fence, facing outward and upward at an angle of 45 degrees. Three or four strands of barbed wire spaced six inches apart are used, but the

NOTE

1. MAT'L FOR NEW ANGLE IS STEEL - GRADE M.

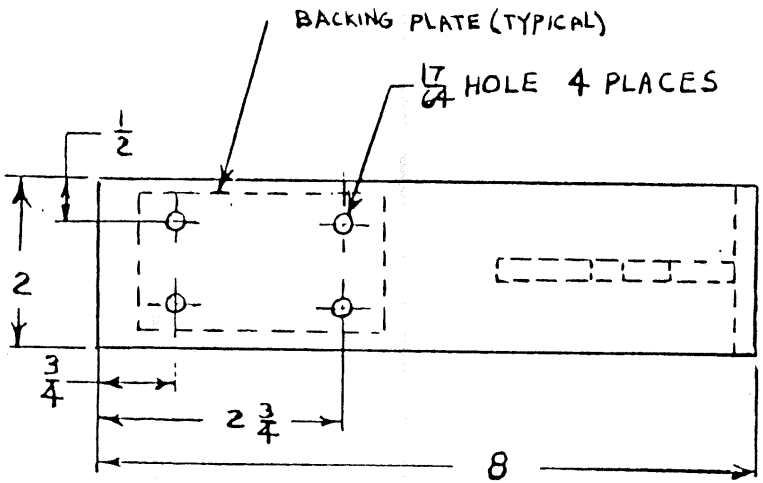


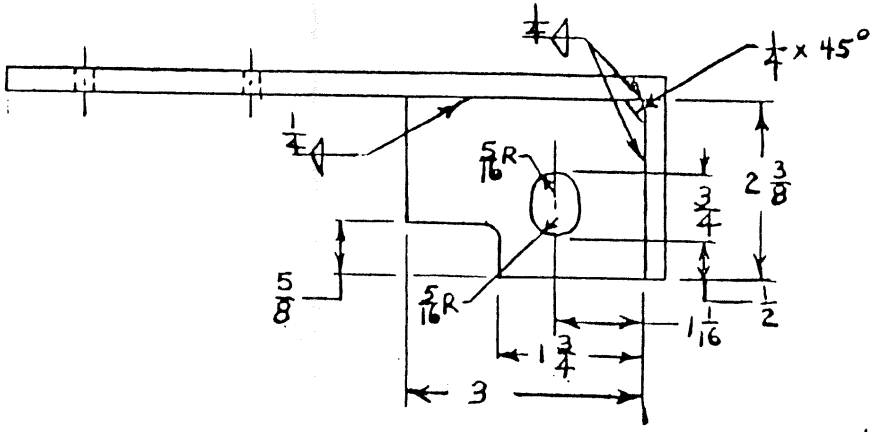
REFERENCE:

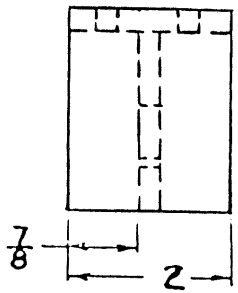
A. - NAVSHIPS DWG. 805-4444649 SMALL ARMS LOCKER ARR. AND DETAIL

MOD. TO SMALL ARMS LOCKER HINGE DESIGN

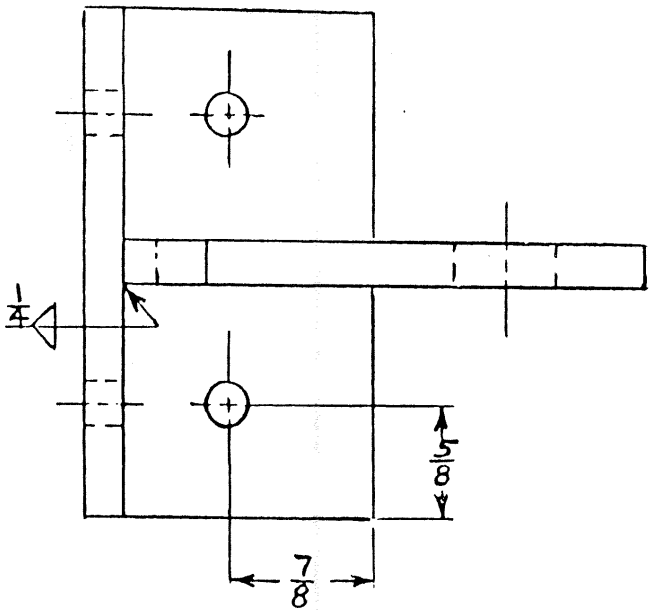
NOTES:
1. HASP MATES WITH SKETCH (4) HASP
2. HASP FOR LOCKERS WITH 2 X 2 ½ ANGLE ON OUTSIDE OF LOCKER.
3. HASP SECURED WITH ¼" STAINLESS BOLTS. BOLT THREADS TO BE DAMAGED AFTER INST'L TO PREVENT REMOVAL.
4. BACKING PL'T ⅛" CRES - AISI 303-314 REQ'D TO REINFORCE BOLT AREA
5. FAYING SURFACES BETWN. ALUM AND STEEL TO BE TREATED I.AW. NAVSHIPS 0901-190-0002
6. HASP MAT'L - ¼" CRES - AISI - 304



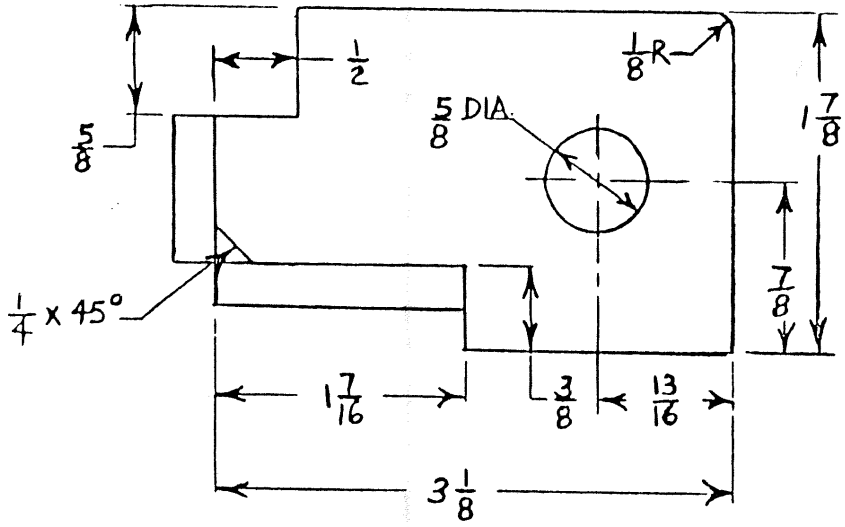


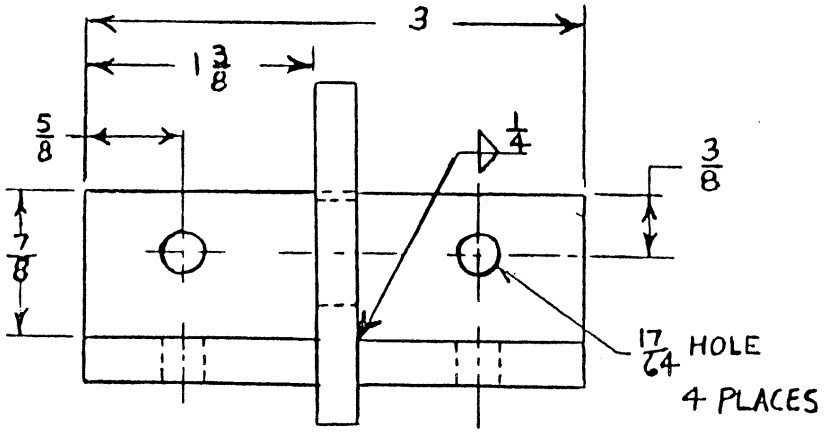


HASP FOR TOPSIDE LOCKER

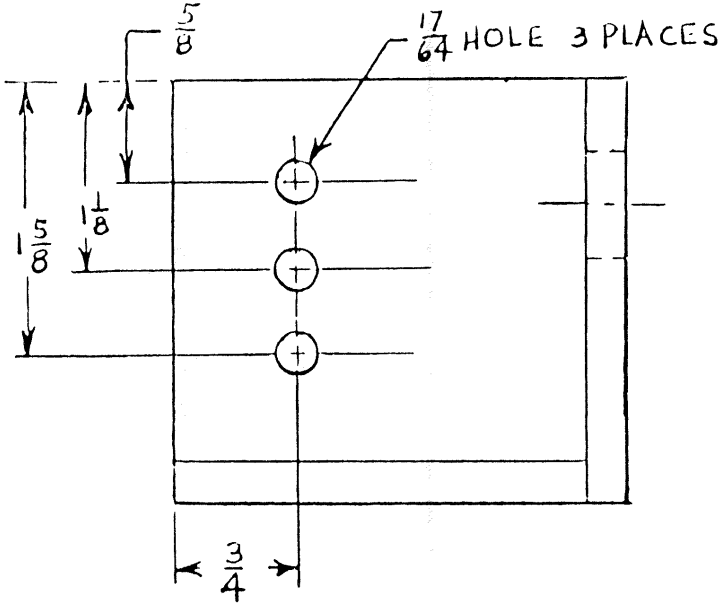


NOTES:
1. HASP MATES WITH SKETCH (3) HASP
2. NOTES 2-6 SKETCH (3) APPLY

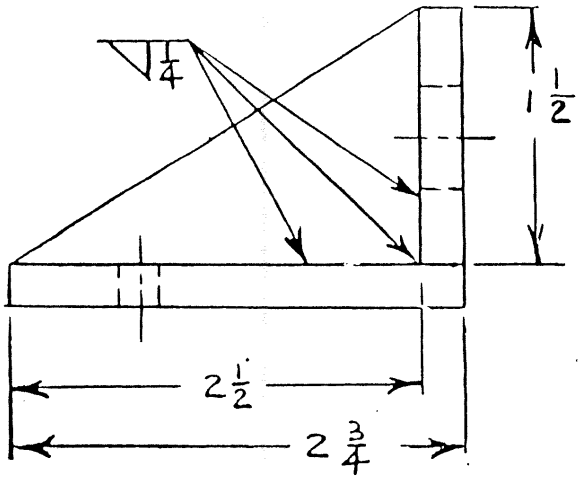


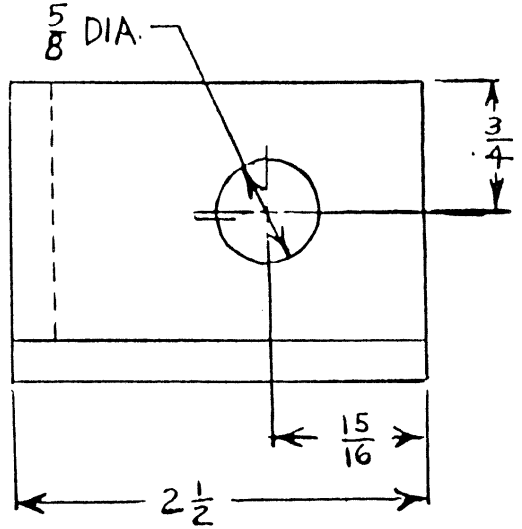


HASP FOR TOPSIDE LOCKER



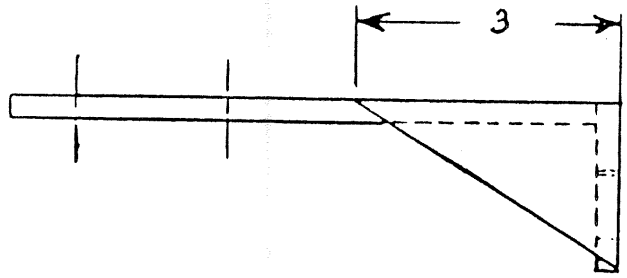
NOTES: 1. HASP MATES WITH SKETCH (6) HASP
2 HASP FOR LOCKER NAVSHIP DWG.
NO. 805-1360275
3. NOTES 3-6 SKETCH (3) APPLY

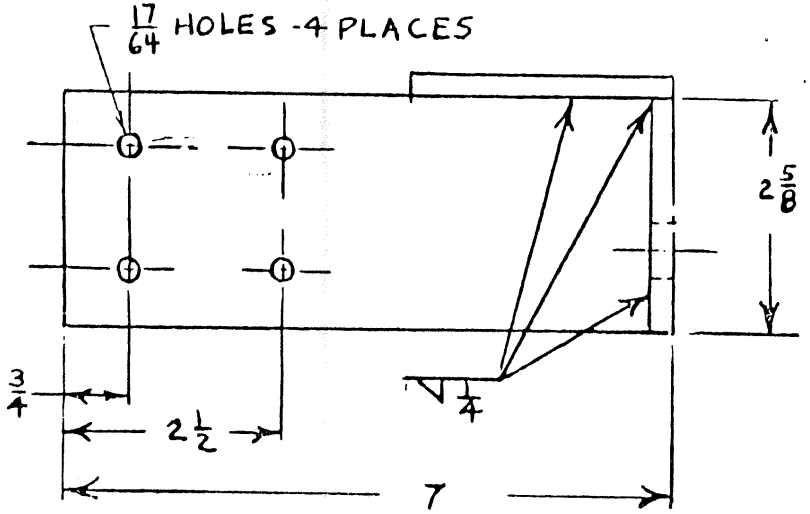


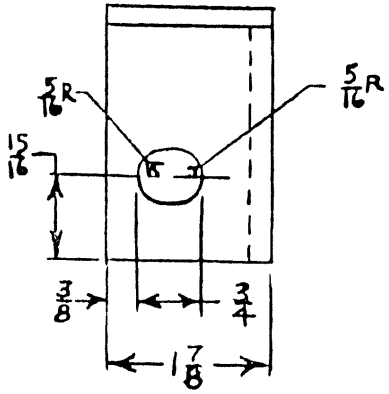


HASP FOR TOPSIDE LOCK

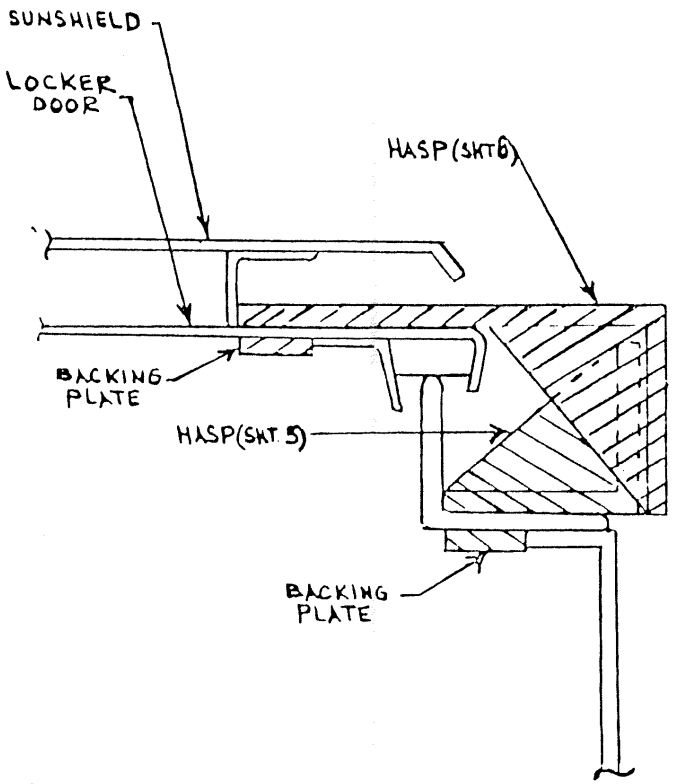
NOTES: 1. HASP MATES WITH SKETCH (5) HASP
2. NOTES 3-6 SKETCH (3) APPLY



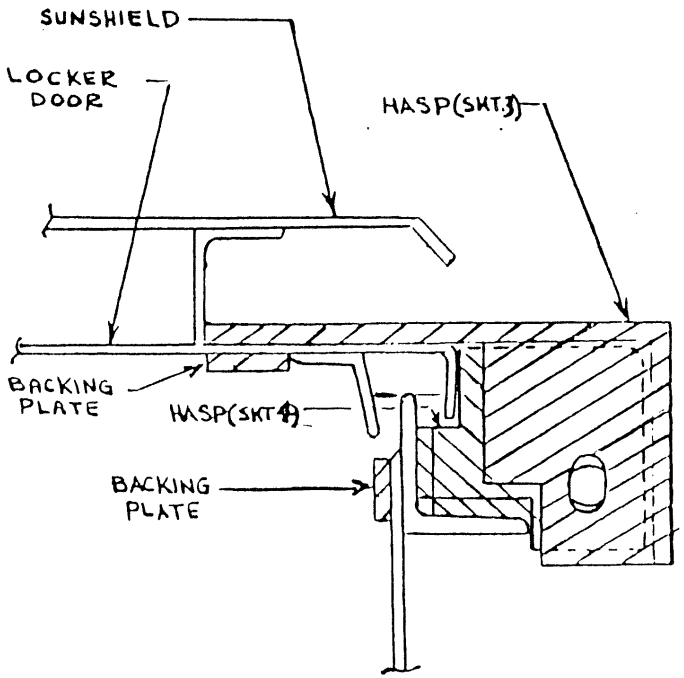




HASP FOR TOPSIDE LOCKERS



LOCKER W/ INTERIOR ANGLE
(DWG. 805-1360275)



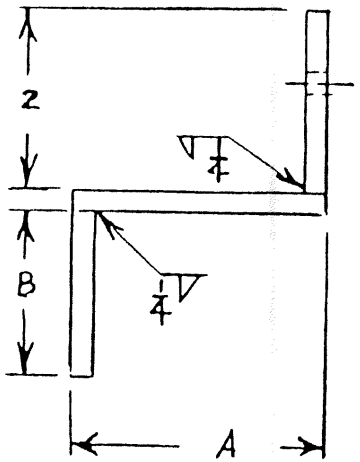
LOCKER W/ EXTERIOR ANGLE

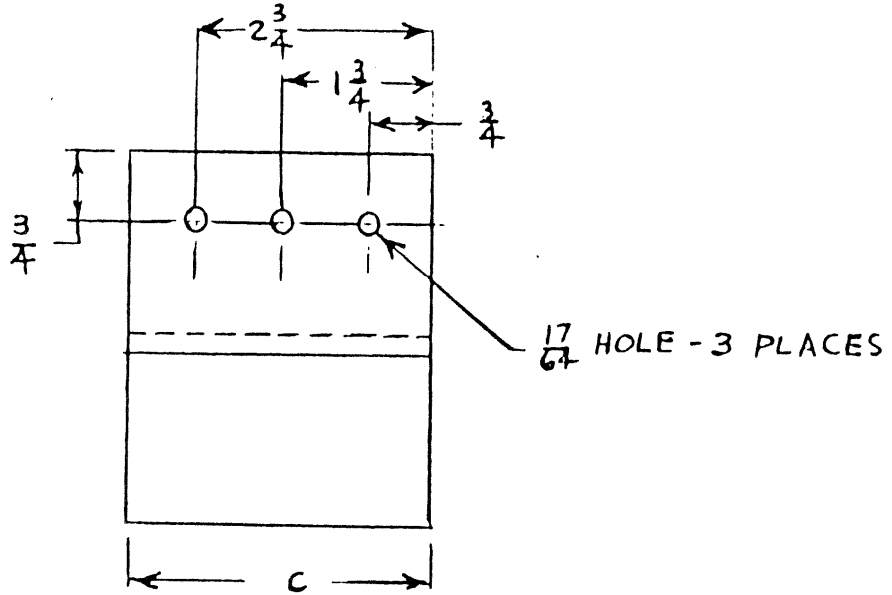
HASP FOR TOPSIDE LOCKER

LOCKER DWG	"A"	"B"	"C" *
805-1360275	$2\frac{1}{2}$	$2\frac{7}{8}$	$3\frac{1}{2}$
All OTHERS	$1\frac{7}{8}$	$2\frac{5}{8}$	$3\frac{1}{2}$

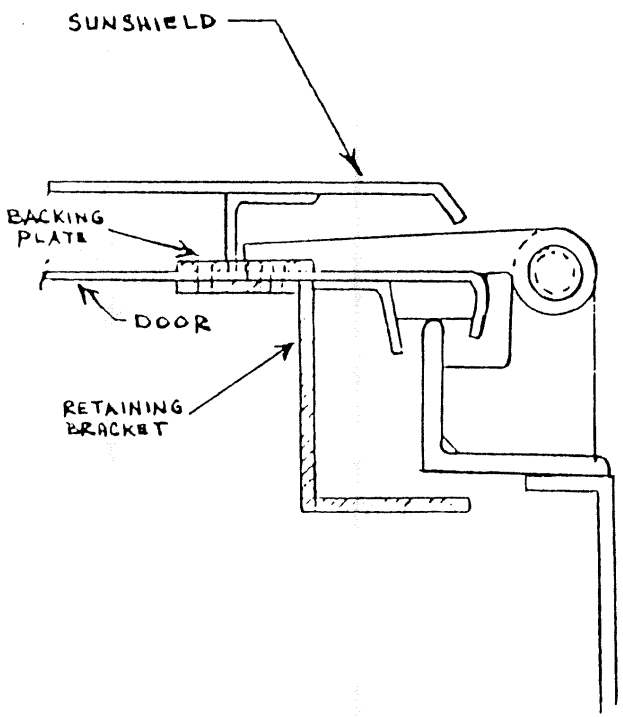
* "C" - MAY BE REDUCED FOR SMALLER LOCKERS

NOTES.
1. INSTALL BRACKET ON LKR. DOOR NEAR HINGE, TWO BRACKETS REQ'D PER LKR.
2. SECURE BRACKET WITH 1/4" STAINLESS BOLTS. DAMAGE THREADS TO PREVENT BOLT REMOVAL
3. BACKING PLT 1/8-1/4" CRES REQ'D TO REINFORCE BOLT AREA
4. WELD 1X1X1/4 ∠ TO INSIDE OF LKR TO MATE WITH BRACKET.
5. FAYING SURFACES BTWN. ALUM & STEEL TO BE TREATED I.A.W. NAVSHIPS 0901-190-0002
6. BRACKET MAT'L - CRES AISI 304

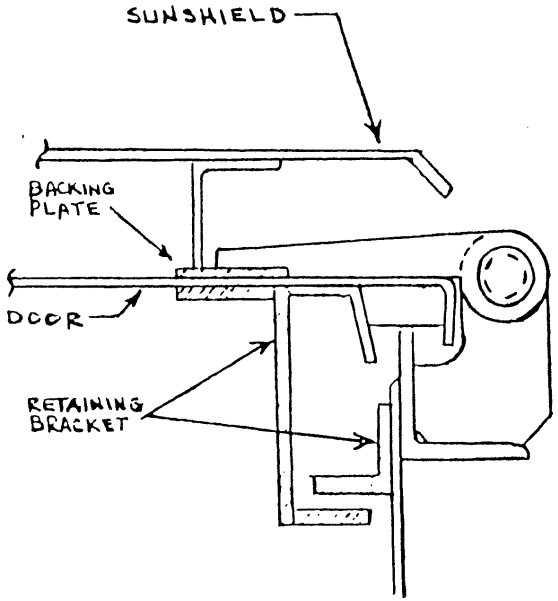




RETAINING BRACKET FOR TOPSIDE LOCKERS



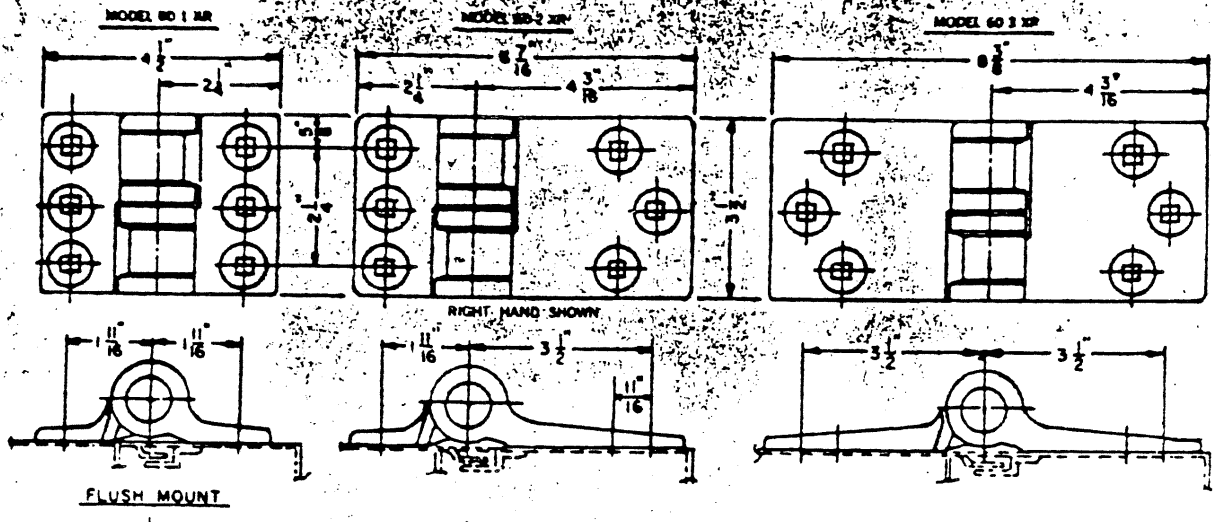
LOCKER W/INTERIOR ANGLE
(DWG. 805-1360275)

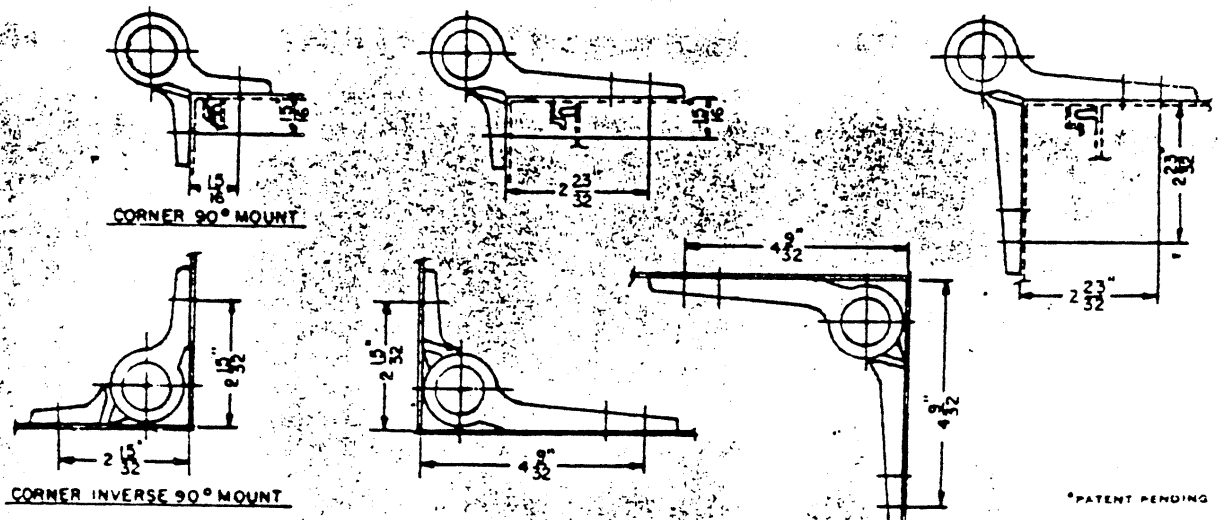


LOCKER W/EXTERIOR ANGLE

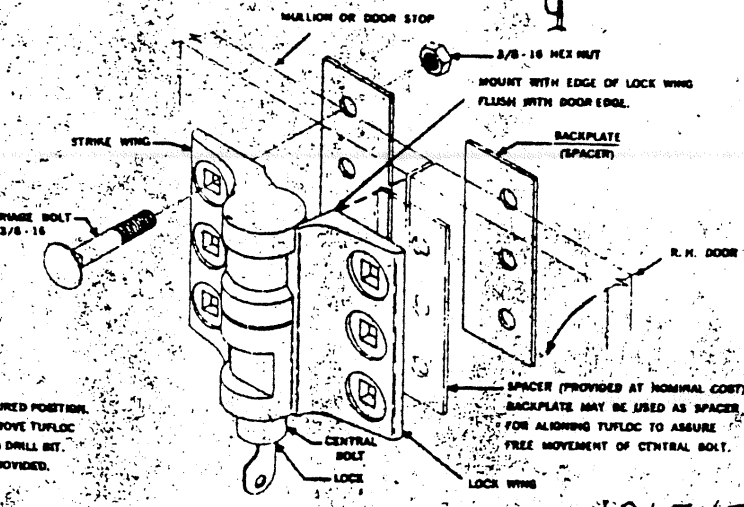
RETAINING BRACKET FOR TOPSIDE LOCKERS

TUFLOC™ MOUNTING SPECIFICATIONS





*PATENT PENDING



NOTE: BEFORE FINAL TIGHTENING OF CARRIAGE BOLTS CHECK CENTRAL BOLT FOR FREEDOM FROM LOCK TO UNLOCK POSITION.

WITH DOORS CLOSED, PLACE TUFLOC INTO DESIRED POSITION. MARK LOCATION OF (6) MOUNTING HOLES. REMOVE TUFLOC AND DRILL MOUNTING HOLES USING "I" (.2570) DRILL BIT. MOUNT TUFLOC WITH 3/8" CARRIAGE BOLTS PROVIDED.

FIGURE A A
FLUSH MOUNT

401548

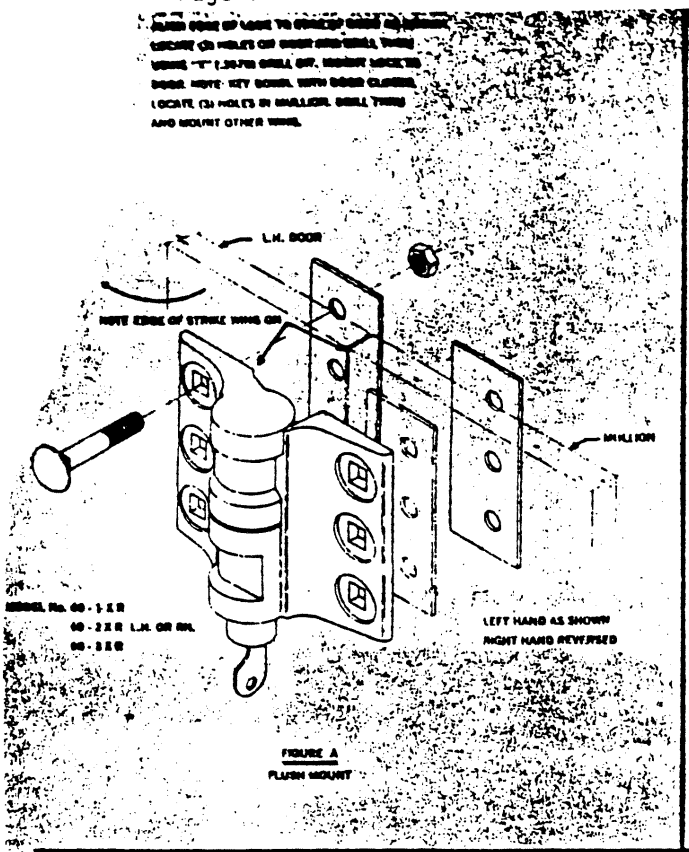


FIGURE A
FLUSH MOUNT

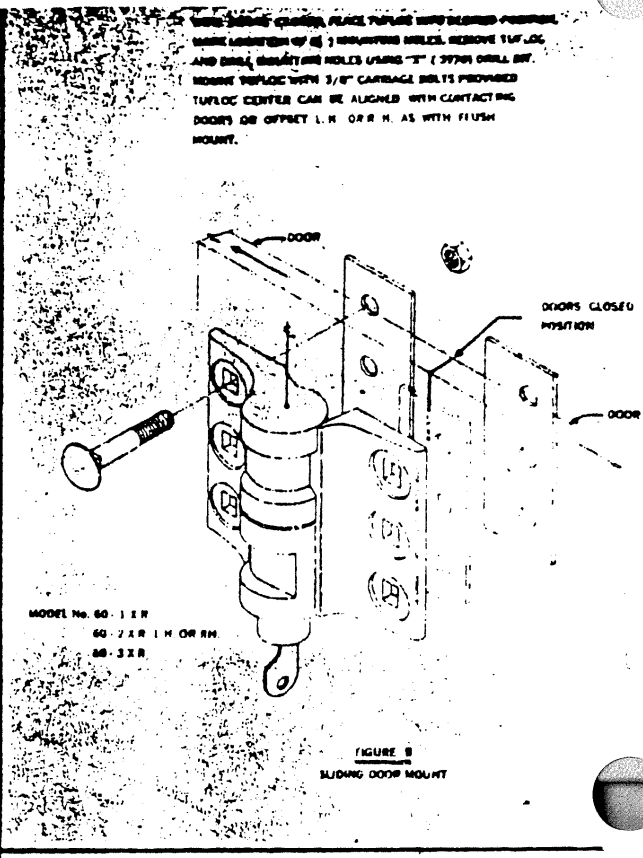


FIGURE B
SLIDING DOOR MOUNT

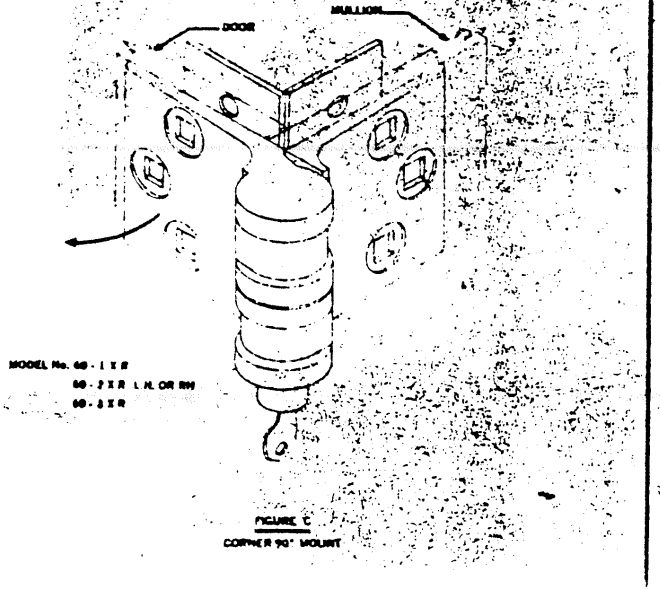


FIGURE C
CORNER 90° MOUNT

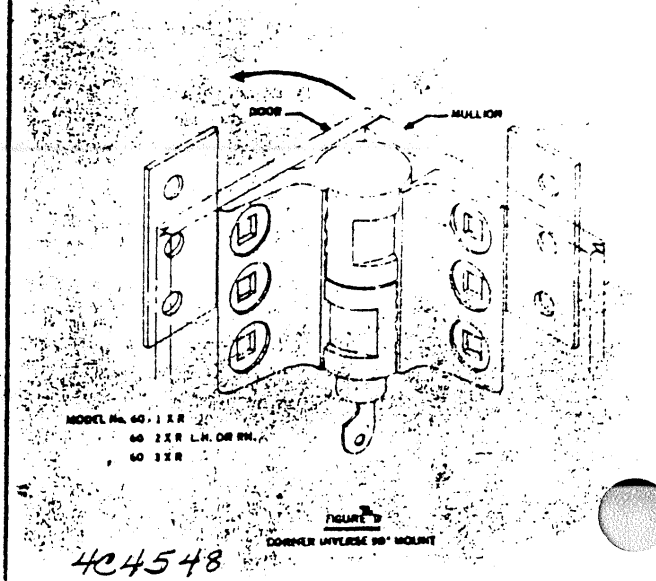


FIGURE D
CORNER INVERSE 90° MOUNT

4C4548

PHYSICAL SECURITY CHECKLISTS

The below checklists are designed to serve as a general guide to be used during the conduct of inspections. They cover the basic security considerations that apply at most, if not all, manned facilities. They may be adapted as need be to apply to the particular requirements of the facility being inspected, including unmanned facilities.

GENERAL CHECKLIST

1. SECURITY PLANNING.

   a. Did security participate in the design and construction stages for the facility?

   b. Are proposed changes in the configuration of the facility which would affect the overall security program coordinated with the security element?

   c. Are the number of personnel and vehicle entrances restricted to the minimum required for operational purposes?

   d. Were the safety and fire protection requirements provided for in the design of the facility?

   e. Are the vital utilities adequately identified and protected?

   f. Have the internal functions and critical areas which have security considerations been identified and strategically located?

   g. Have the basic physical control measures been provided for in the leasing arrangements for a facility located in a commercially-owned building?

   h. Have contingency plans been developed to safeguard life and property in the event of all emergencies?

   i. Have the contingency plans been tested?

2. PERIMETER CONTROLS.

   a. Is the perimeter of the facility defined by a fence or other type of physical barrier?

b. If a fence is used, does it meet the minimum specifications for security fencing?

c. If building walls and roofs form a part of the perimeter barrier, do they provide a degree of security equivalent to that provided by chain link fence?

d. If a building forms a part of the perimeter barrier, does it present a hazard at the point of juncture with the perimeter fence?

e. Are openings such as culverts, tunnels and manholes for sewers and utilities which cross the fence line properly secured?

f. Are the number of perimeter entrances and gates restricted to the minimum required?

g. Are all perimeter entrances equipped with secure locking devices and locked when not in active use?

h. Is the perimeter of the facility protected by adequate lighting?

i. Is there a dependable source of power for the lighting system, including an emergency power supply?

j. Are intrusion detection devices used for perimeter protection purposes?

k. Are the gates properly controlled both during and after normal duty hours?

3. BUILDING CONTROLS.

a. Are entrances, including potential entrances, adequately secured?

b. Have miscellaneous openings into the buildings been secured?

c. Are the doors installed properly, e.g., frame, hinges, panels?

d. Are the doors properly constructed or covered with sheet steel?

e. Are glass panels afforded added protection?

f. Are the overhead doors secured properly?

g. Are windows, including the frames, securely fastened?

h. Are utility entrances properly secured?

i. Are potential access points on the roofs secured?

j. Are ventilating shafts, vents or ducts which are large enough to provide an entry into the building equipped with screening or bars?

k. Are walls of solid construction?

4. INTERIOR CONTROLS.

a. Have the critical areas in the facility been identified?

b. Are the access controls to the critical areas adequate?

c. Are the Government funds properly protected?

d. Have written procedures been prepared by the fund custodian outlining action to be taken in the event of a robbery?

e. Have the contingency plans been tested to insure their effectiveness?

f. Are the security controls within the fund activity periodically inspected?

g. Is the fund activity strategically located within the facility?

h. Are administrative safeguards observed in the handling and transfer of funds?

i. Are the funds stored properly and supplemental controls provided for as necessary?

j. Is the fund storage room properly constructed?

k. Are controlled substances, dangerous drugs and narcotics properly stored and knowledge of the combination restricted?

l. Are small arms and ammunition stored only in secured, manned facilities?

m. Are the weapons storage areas properly constructed?

n. Are the storage areas aboard ships adequate?

o. Are the small arms kept in locked racks or in an approved Class 5 storage container?

p. Have areas containing pilferable equipment and supplies been pinpointed?

q. Have adequate control measures been established to help in the prevention of pilferage?

r. Is there a close working relationship between the security and property accountability offices on matters involving the loss and theft of Government property?

s. Are reports of lost or stolen property submitted promptly to the security office?

t. Is the security office apprised of unexplained shortages uncovered by the annual physical inventories?

u. Are protective devices used to secure office equipment in place?

5. LOCKS AND KEYS.

a. Has locking hardware been properly selected and applied at the facility?

b. Does the facility have a master-keyed locking system supplied by one manufacturer?

c. Is the locking hardware of the medium or heavy duty type and have interchangeable cores?

d. Are high-security key padlocks in use at the facility?

e. Are electro-mechanical door devices used for the purpose of controlling access to selected areas?

f. Are the number of keys issued kept to a minimum?

g. Are unissued keys properly protected?

h. Is adequate accountability maintained for all keys?

i. Has a key control official been appointed?

6. GUARDS.

a. Is there a guard force at the facility?

b. If not, is there a need for guard coverage?

c. Did the cognizant security element participate in the preparation of the specifications for the guard contract?

d. Are qualified guards assigned to the facility?

e. If required, do the contract guards have ghe requisite security clearances?

f. Are the contract guards armed and, if so, have the requirements of DOT Order 1620.1A pertaining to the use of weapons been incorporated into the guard contract?

g. Is there a sufficient number of guards assigned to the facility?

h. Are the fixed posts properly located?

i. Are interior patrols conducted after normal duty hours?

j. Are the guard orders adequate and observed?

k. Are the guards properly supervised?

l. Are incident reports promptly submitted to the security element?

7. INTRUSION DETECTION SYSTEMS.

a. Are intrusion detection devices used to supplant or supplement the guard forces.

b. Is the response time adequate?

c. Is the alarm system adequately "secured" through the combination of technological and physical security measures?

d. Are the signed lines properly protected?

e. Are alarm systems used to maximum advantage?

f. Are records kept of all alarm situations, including the reasons for and the findings?

8. VII DESTRUCTION EQUIPMENT.

   a. Are authorized methods used for the destruction of classified material?

   b. Is the destruction process complete with no possibility of reconstruction?

   c. If used, do the shredders cut the material into the required dimensions?

   d. Is the aperature size of the security screen in the pulverizer of the prescribed size?

9. STORAGE EQUIPMENT.

   a. Are only approved security containers used for the storage of classified material?

   b. Has a schedule been established for the orderly replacement of existing non-approved containers?

   c. If applicable, are vaults and/or strongrooms constructed in accordance with the established criteria?

   d. Are the vault doors equipped with an emergency escape and relocking device?

   e. If used, are the combination padlocks of the approved type?

   f. Is maximum utilization made of the storage containers?

10. SURVEYS AND INSPECTIONS.

   a. Has an initial survey been conducted at the facility and other proposed security controls implemented?

   b. Is a survey report for that facility on file in the security element?

   c. Is this a Category 1, 2 or 3 facility? (Category _____.)

   d. Has the facility been inspected in accordance with the established schedule?

   e. Have deficiencies noted during the inspection been corrected?

   f. When warranted, have follow-up inspections been conducted?

g. Has assistance been obtained from non-security functions in meeting the inspection requirements? If so, have such reports been properly reviewed and acted upon?

11. INCIDENT REPORTING.

a. Are incidents involving the theft, loss or malicious damage of Government property promptly reported to the security element?

b. Are the incident reports accurate and complete?

c. Are reports submitted in the required format?

d. When required, is notification of the incident furnished to the FBI and/or the local law enforcement agency?

e. Is the headquarters security element advised of significant incident and furnished required statistical data reflecting the theft/loss experience during the established timeframe?

WAREHOUSE CHECKLIST

1. Is there a specific procedure in effect that assures strict accountability of all property? (On separate sheet, show value of last inventory.)
2. Are the records of this activity subjected to periodic audits?
3. Are sufficient and comprehensive physical inventories conducted?
4. Are inventories conducted by disinterested activity personnel?
5. Is fixed and real property accounted for?
6. Are stock record or bin cards maintained?
7. Are stock levels on these cards verifiable through records of incoming stock?
8. Are issues recorded on these cards indexed to specific requisitions? (Voucher No's.)
9. Are investories recorded on these cards?
10. Is there excessive use of reports of survey?
11. Is there a specific and secure procedure for the receipt of incoming property?
12. Are there any weaknesses in the present system for the physical unloading and storage of merchandise?
13. Are delivery personnel required to produce a Bill of Lading or other listing of the delivery?
14. Is an accurate tally conducted prior to acceptance?
15. Are delivery records checked against requisitions or purchase orders?
16. Is acceptance of deliveries limited to specific personnel?
17. Are incoming shipments carefully checked for signs of pilferage, damage, etc.?
18. Are shipping and receiving platforms free of trash and are shipments neatly stacked for proper observation and counting?
19. Are unauthorized persons kept from storeroom/storage areas?
20. Is a current personnel access list maintained?
21. Are supplies adequately protected against pilferage?
22. Are adequate protective measures afforded open storage?
23. Is material in open storage properly stacked, placed within, away from, and parallel to perimeter barriers, to provide unobstructed view by patrol personnel?
24. Are adequate locker and "break area" facilities provided for employees?
25. Is there a secure place to keep broken cases of damaged merchandise to prevent pilferage?
26. Is there a secure room or container for the safekeeping of sensitive items?
27. Are employees permitted to carry packages in and out of work areas?
28. Are provisions made for parking privately owned vehicles to insure that they are not parked in an area offering an opportunity to remove items from the building to the vehicle undetected?
29. Are trash collectors permitted in the building? (Janitorial help.)

30. If so, are trash containers inspected to assure no supplies are secreted in the containers?

31. Is there a specific procedure in effect for the issue and/or shipping of property?

32. Are there any weaknesses in the present system for the physical issue or shipment of property?

33. Are receivers required to receipt for the goods?

34. Are signature cards used for all authorized receiptors?

35. When issues are made by shipment, is there a means to verify their arrival at the requesting facility?

36. Are shipments or deliveries receipted to the carrier or the person making the delivery?

37. Are adequate controls maintained over property prior to issue?

38. Is responsibility for items fixed?

FUND ACTIVITY CHECKLIST

1. Is the fund activity adequately guarded?

2. Have adequate precautions been taken to prevent unauthorized entrance after duty hours?

3. Have security measures been coordinated with the security element?

4. Is the fund activity equipped with adequate facilities for the storing and safeguarding of public funds and documents?

5. Do the safeguards employed during normal operations preclude loss, substitution, or pilferage of public funds and documents?

6. Are vaults or safes accessible at any time to unauthorized persons?

7. Are unauthorized persons excluded from the working areas of the office by means of railing or counter?

8. Are money exchanging windows situated so as to prevent unauthorized access to funds? (If not, explain on separate sheet.)

9. Is cash in excess of current disbursing needs promptly deposited to the credit of the Treasurer of the United States?

10. Are internal office procedures established to provide controls on all undelivered and returned checks?

11. Is there a central point for their receipt, holding, and final disposition, with responsibility therefor charged to a specific individual?

12. Is the cashier provided with a separate working space or properly inclosed cage or room with a window for paying and receiving?

13. Is a cash drawer with key lock, or a field or similar safe, provided for safeguarding funds and vouchers during temporary absence of the clerks?

14. If more than one person in the office has cash in his possession, is each person provided with a separate and secure receptacle for such monies?

15. Are receipts taken for all funds entrusted to the cashier and receipts given the cashier for all funds returned or valid vouchers accepted?

16. Is there a procedure for unannounced verification of cash on hand?

17. Do current records indicate that such verifications are being made on an unannounced basis at least once each quarter?

18. Is a detailed record maintained of daily settlement of cash transaction between disbursing officer and cashier(s) or deputy and cashier(s)?

19. Is positive identification of the payee made prior to any cash payments?

CONTROLLED SUBSTANCE CHECKLIST

1. Does the location of the room/area afford adequate protection?
2. Is the room/building that houses the narcotics of permanent construction?
3. Are bulk narcotics/controlled drugs stored in a vault or similar protective storage?
4. Is there an authorized narcotics cabinet/chest (hospital ward)?
5. Is the vault/safe/cabinet kept securely locked when not in use?
6. Are responsible personnel in close vicinity to assure protection?
7. If narcotics are stored in a small moveable safe or the like, is the safe adequately secured to a permanent part of the storage room or building?
8. Are procedures established to insure strict accountability and control of narcotics and controlled drugs?
9. Is a narcotic and controlled drug register maintained?
10. Does it contain narcotic and controlled drug inventory?
11. Does it contain a narcotic and controlled drug record?
12. Is the register maintained properly?
13. Is a separate record prepared for each drug or alcoholic content?
14. Is a joint inventory taken by the responsible person going off duty and the person coming on duty?
15. Is the balance on hand recorded in the appropriate column by both responsible persons?
16. Is the register secured and available only to authorized personnel?
17. Is the box heading of each record completed in its entirety, i.e., ward number, date, correct name of the drug, accountable unit of measure, and balance on hand?
18. When a drug is dispensed, is the complete information recorded as to disposition, i.e., day, hour, patient's name, initial and last name of doctor who ordered the medication, etc.?

19. When a unit of narcotic or controlled drug is accidently destroyed, damaged or contaminated, is a record of the fact entered on the record?

20. When accountable drugs are issued to a ward, are entries made by the pharmacy representative on the appropriate form, i.e., the day, hour, amount of drugs, and new balance?

21. Are corrections of errors in the drug register in accord with current regulations?

22. Have there been any reports of a loss, theft, or unaccounted for drugs within the past 12 months?

23. Is an intrusion detection device/system installed?

Guide to a facility protection plan

July 1976

Federal
Protective
Service

F

TABLE OF CONTENTS

TABLE OF CONTENTS CONTINUED

DATE: _____

*LISTING OF PERSONNEL TO BE CONTACTED IN EVENT OF EMERGENCY

Name	Room Number	Business Phone	Home Phone
DESIGNATED OFFICIAL			
DEPUTY DESIGNATED OFFICIAL			
COORDINATOR			
CHIEF WARDEN			
BUILDINGS MANAGER			
EMERGENCY			
BUILDING GUARD OFFICE			
GUARD POST			
Other			

*Update as necessary.

Local Police Dept.

Local Fire Dept.

Ambulance Service

Health Unit

Army Explosive Ordnance Disposal Unit

DATE: _____

*ROSTER OF ORGANIZATION OFFICIALS

Official	Name, Position and Agency	Room and Telephone
**Designated Official		
Deputy Designated Official		
Buildings Manager		
Personnel Movement Officer		
Medical Officer		
Fire Marshal		
Utilities Officer		
Bomb Reconnaissance Officer		
***Welfare Officer		
***Radiological Officer		
***Supply Officer		

*Update as necessary.

**An alternate shall be selected for each Organization Official.

***Do not include these officials in the plan if the facility does not have an approved civil defense emergency shelter.

DATE: _____

APPROVAL

The Facility Protection Plan for (Building Address) has been coordinated with and approved by officials of tenant agencies.

_____ (Designated Official)

_____ (Buildings Manager)

_____ (Tenant Agency Official)

_____ (Tenant Agency Official)

_____ (Tenant Agency Official)

_____ (Tenant Agency Official)

Office responsible for plan preparation, clarification, updating, and changes:

Agency	Office	Rm. No.	Tel. No.

CHAPTER 1. GENERAL

1. GENERAL. The Federal Government has an inherent responsibility for minimizing danger to life and property arising from the effects of bomb threats, bombs, enemy attack, fire, explosion, earthquake, serious weather disturbances and other disasters affecting a Federal building. To cope with these effects, the General Services Administration requires development of a protection plan in accordance with FPMR, Chapter D, subpart 101-20.5, Physical Protection; and HB, Disaster Control and Civil Defense in Federal Buildings (PBS P 2460.1A), and HB, Physical Protection, chapter 11, (PBS P 5930.2A).

2. Authority. The authority of the General Services Administration for the protection of life and property in federally-owned and occupied buildings, and its responsibilities for emergency preparedness program in such buildings, is derived from statutes and Executive Orders.

3. Applicability. The responsibilities and procedures recommended in this Model Plan apply to all property under the charge and control of the General Services Administration and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations.

4. Provisions of the Facility Protection Plan.

a. Federal Property Management Regulations Chapter D, subpart 101-20.1 (Building Operations, Maintenance, Protection and Alterations) applies to the closing of buildings to the public when:

(1) Emergency situations make it reasonably necessary to ensure the orderly conduct of Government business. The decision to close the property shall be made by the designated official under the Facilities Protection Plan.

(2) Conduct on the property creates loud or unusual noise; reasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots; otherwise impedes or disrupts the performance of official duties by Government employees; or prevents the general public from obtaining the administrative services provided on the property in a timely manner. THE DESIGNATED OFFICIAL UNDER THE FACILITIES PROTECTION PLAN SHALL BE RESPONSIBLE FOR ENFORCING THIS RULE.

b. A current complete copy of the Plan will be kept on file by all personnel shown on pages iii and iv and all tenant agency officials. The Buildings Manager will forward three copies to the Federal Protective Service Division, Public Buildings Service, GSA Region 3, 3PSS. The Plan will be available for inspection by GSA and by tenant agency officials. The Plan will include a

record of its approval by the appropriate agency officials and shall be updated as necessary to insure that it is current at all times.

c. The basic provisions of the Plan will be made known to all building occupants by:

(1) Posting alarm signals on bulletins boards.

(2) Posting evacuation routes on bulletin boards, corridor intersections and office exits.

(3) Posting listings of [illegible] Protection Organization personnel on bulletin boards. (Pages iii and iv)

(4) Distributing emergency instructions to all employees.

CHAPTER 2. ORGANIZATION

1. Responsibilities.

   a. The establishment of the Protection Organization in the (Name or Address of Building) is a joint responsibility of all tenants. (Name of Agency) is the agency having the largest number of employees assigned to this building, is considered the primary tenant, and therefore, is responsible for providing the direction for the development of the Self-Protection Plan and for staffing and training of the Organization. Personnel for the Organization will be recruited on an equitable basis from among all the tenants.

   b. To the extent possible, GSA will install and maintain protective equipment, such as warning devices, alarm systems, and firefighting apparatus, and will promote training for building operations employees and other employees in equipment use.

2. Advisory Committee. An advisory committee will be established to assist in the development of various phases of the Plan. The committee will consist of one representative from each tenant agency.

3. Designated Official. (Name of Official), the highest ranking official of the primary occupant agency, will be the Designated Official for the building. (Can be an alternate high ranking official, designated in advance by agreement of occupant agency officials.)

4. Buildings Manager. The Buildings Manager is responsible for providing leadership, assistance, and follow-up to ensure establishment and continuity of the Plan. He will provide information and guidance, advice on establishing the Organization, and he will assist the designated official in recruiting qualified personnel for technical services such as utilities control and for making arrangements for training of Organization personnel.

5. Designation of other Organization personnel.

   a. Each tenant agency will provide the personnel to staff the Organization for the building in proportion to its share of the total Federal employment in the building. The Designated Official will confer with the appropriate official of each tenant agency and arrange for the designation of a principal and alternate for each of these positions: Deputy Designated Official, Bomb Search and Reconnaissance Officer, Personnel Movement Officer, Medical Officer, Fire Marshal, and Utilities Officer. (Refer Figure 2-2) Depending on availability of rescue personnel such as Fire Departments, consideration should also be given to the need for a rescue team.

b. Each of the Organization officials will be designated in a letter signed by the Designated Official and countersigned by the chief official of the agency in which the designee is employed. The Designated Official will retain a copy of each letter of designation.

ORGANIZATION CHART

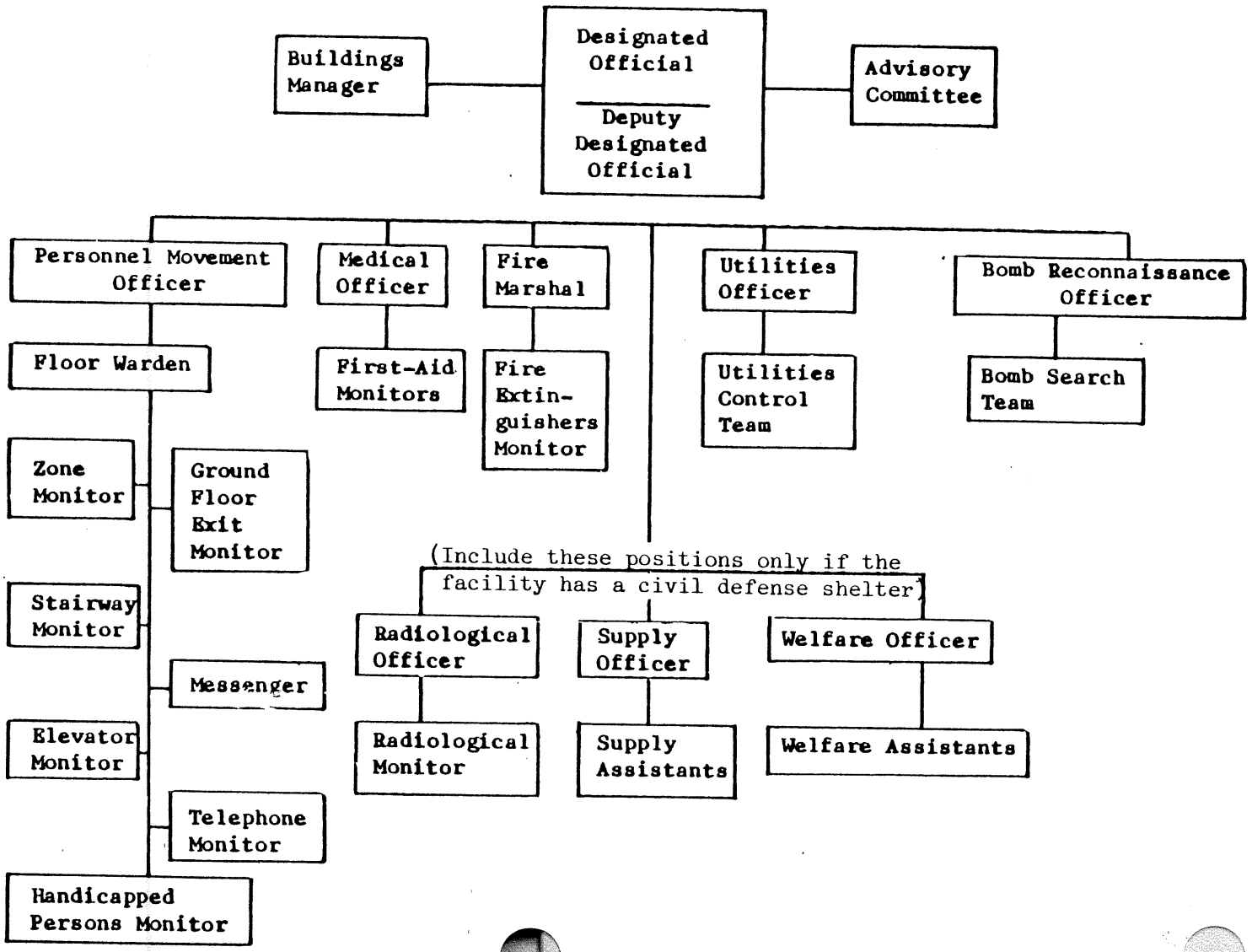


Figure 2-1

TYPICAL STAFFING REQUIREMENTS

BUILDING DESCRIPTION:

Location	Address
Construction	Fire resistive-Heavy Timber-Noncombustible-Ordinary-Wood Frame.
GSA Building Number	XXXXXX
Number stories	XX
Net area	sq. ft.
Occupancy	Office-Storage-Special
Number occupants	000
Total FSPO Support Assignments	00
Total FSPO Alternate Assignments	00

SUPPORT PERSONNEL:

First through xxxx Floors

Number

- Floor Warden
- Room Monitors
- Exit Door Monitors
- Elevator Monitor
- Messenger
- Telephone Monitor
- First-Aid Monitors
- Fire Extinguisher Monitors
- Handicapped Persons Monitor
- Stairway Monitors
- Zone Monitors
- Wing Monitors

Figure 2-2

Utilities Control Team

X persons per building -- Assigned as needed.

*Welfare Assistants

X persons per building -- Assigned as needed.

*Radiological Monitors

X persons per building -- Assigned as needed.

*Supply Assistants

X persons per building -- Assigned as needed.

An alternate shall be selected for each support position.

*Personnel should be assigned to these positions only if the facility contains a civil defense shelter.

Figure 2-2

6. Building occupants. Each supervisor will acquaint his employees with the alarm signals and emergency instructions. Each employee is expected to react to alarms and direction by Organization personnel during an emergency. The employee must follow directions of and cooperate with Organization personnel.

7. Basic functions. The Organization as shown in Figure 2-1 will perform the following functions:

a. Firefighting and evacuation of building occupants. This function provides for the planned and directed evacuation of all building occupants in the event of an emergency. Also, it provides for the fighting and control of fires before the arrival of local fire-fighting forces. It is performed by the firefighting and evacuation group under the direction of the Firefighting and Personnel Movement Officer who are assisted by floor wardens and their assistants.

b. First-aid. This function provides for emergency medical treatment by personnel trained in administering first-aid. It is performed by the Medical Officer who is assisted by First-Aid Monitors.

c. Utilities control. This function provides for control of utilities in the building in the event of an emergency. It includes the control of all electrical and mechanical equipment; water, gas and steam valves and conduits; power switches; ventilation and refrigeration devices; and any other such equipment in the building. Personnel employed in the maintenance and building operations should be assigned to this function. It is performed by the utilities control group under the direction of the Utilities Officer who is assisted by the utilities control team.

8. Succession to command. To provide continuity, certain persons are designated to succeed to command should the Designated Official be unable to discharge the duties and responsibilities of that position. The succession to command is as follows:

1. Deputy Designated Official
2. Personnel Movement Officer
3. Chief (or first floor) Warden
4. Fire Marshal
5. Bomb Reconnaissance Officer
6. Utilities Officer

CHAPTER 3. DUTIES AND RESPONSIBILITIES

1. Designated Officials's Duties. The Designated Official is responsible for developing the Plan to protect life and property and to minimize damage in the event of a *(civil defense emergency or other) disaster; for coordinating such planning with the Buildings Manager, tenant agency officials; and (the local civil defense director;) for selecting, organizing, and training an adequate staff to conduct the emergency operations required by the facility's Plan (and for directing and supervising the activities of the building occupants during an enforced stay in the shelter within the facility.)

The Designated Official performs at least the following duties:

a. He insures that the basic provisions of the Plan are disseminated to all persons employed in the building.

b. He requests the Buildings Manager to assist in planning for, obtaining, and installing necessary alarm systems; and in recruiting or selecting qualified emergency service personnel.

c. He establishes and reports to a control point from which the activities of the Organization may be directed in an emergency.

d. He maintains liaison and cooperates with the principal officers of the tenant agencies, or their designees, on problems arising in the selection and training of tenant agency employees for the Organization.

e. He arranges for posting on appropriate bulletin boards (or otherwise publicizes within the building) a roster of Organization personnel who have responsibilities for (inshelter or other) emergency operations.

f. He takes all necessary actions to insure that the facility's Organization operates safely and efficiently in emergencies.

g. He exercises command responsibility for the orderly movement of all personnel in the building (including non-tenants) in accordance with the Plan.

h. He maintains liason with (the local civil defense director,) the local fire and police departments.

i. He insures that appropriate training courses are set up and that arrangements are made for obtaining assistance from (the local civil defense organization,) the Red Cross, local fire and police departments, and other sources, as required, to train the Organization staff.

j. With the approval and cooperation of his agency, the Buildings Manager, and the building owner, he coordinates arrangements for and directs (civil defense,) fire and bomb evacuation drills.

k. He arranges for and supervises the storage of required supplies and equipment in the facility (shelters).

l. He conducts periodic inspections of (shelters in) the facility.

(m. He directs all shelter management operations when fallout shelters in the facility are occupied.)

(n. He works closely with and cooperates with the local or state civil defense director in all matters involving the facility's Plan, Organization, or operations.)

(o. He assesses the nature and extent of damage resulting from enemy attack and reports this to the local civil defense director.)

*NOTE: All references to civil defense operations and responsibilities are contained in brackets. If the facility does not contain a civil defense shelter, the brackets and enclosed words should be eliminated.

2. Deputy Designated Official (or Coordinator). The Deputy Designated Official serves as the principal assistant to the Designated Official and acts for him in his absence. The Deputy performs such duties as the Designated Official may assign. The Designated Official may assign to the Deputy the responsibility of coordinating the training of Organization personnel, including arranging for instructors, obtaining appropriate training materials, arranging training schedule, etc. During emergencies he reports to the control center.

3. Personnel Movement Officers. The Personnel Movement Officer is responsible for supervising and expediting the planned and controlled movement of all building occupants in an emergency. Under the general direction of the Designated Official, the Personnel Movement Officer serves as head of the Personnel Movement Service and performs the following duties:

a. Plans personnel movement routes and establishes movement procedures to effect the personnel movement provisions of the Plan.

b. Assures that all Organization personnel responsible for occupant evacuation, conduct an evacuation route search for bombs or suspicious items BEFORE any occupants are allowed to pass through public areas.

c. Assigns and trains Floor Wardens and related personnel as required.

d. During drills and actual emergencies, supervises and directs movement of personnel within, (into,) or out of the building as required by the building protection plan.

e. Assures that all building occupants, including members of the Organization, comply with procedures indicated by the alarm signals as specified by the Plan.

f. During emergencies, he reports to the Control Center.

4. Floor Warden. Under the direction of the Firefighting and Personnel Movement Officer, the Floor Warden supervises firefighting and expedites the evacuation of personnel from his floor. His duties include:

a. Assuring that evacuation routes are clearly identified, are posted on the bulletin board, corridor intersections and office exits, and are made known to the regular occupants of the floor.

b. Assuring that the evacuation procedures are known to all regular occupants of the floor.

c. Directing the orderly flow of personnel, during drills or actual emergencies, along the prescribed evacuation routes.

d. Immediately establishing a new route of evacuation if a bomb or a suspicious item is discovered along the normal route of evacuation. Insuring that no part of a straight line route is used if a suspicious item is contained within a corridor, stairwell, wing, etc.

e. Assuring that fire extinguisher monitors know their stations, locations of firefighting equipment in their area of responsibility and the alarm signals which direct them to their stations.

f. Coordinating the activities of stairway monitors, elevator monitors, telephone monitors, zone monitors, messengers, handicapped persons monitors, fire extinguisher monitors, and first aid monitors.

g. Maintaining a current roster, which is posted on the bulletin board, of personnel with evacuation assignments by listing names, emergency assignment, room number, and telephone number, and keeping the Firefighting and Personnel Movement Officer informed of changes in the roster.

h. Maintaining a roster of physically handicapped personnel regularly on the floor and making provisions for their evacuation in an emergency.

i. Immediately reporting fires on his floor to the Designated Official.

j. Reports to the Control Center after evacuation has been completed.

5. Zone Monitor. Under the direction of the Floor Warden, the Zone Monitor supervises and expedites the evacuation of personnel from his part of the floor. His duties include:

a. Assuring that evacuation routes are clearly identified and are made known to the regular occupants in his part of the building.

b. Directing the orderly flow of personnel, during drills or actual emergencies, along the prescribed evacuation routes in his part of the building.

c. Immediately establishing a new route of evacuation if a bomb or suspicious item is discovered along the normal route of evacuation. Insuring that no part of a straight line route is used if a suspicious item is contained within a corridor, stairwell, wing, etc.

d. Appointing column leader to lead personnel along the prescribed routes to an area specified by the Floor Warden.

e. Assuring that all personnel have vacated his area of the floor when this is required.

f. Assuring that rooms are vacated, windows and doors are closed, and electrical appliances are turned off in his part of the building during fire evacuations.

g. Windows and doors are to be left open and lights remain on during bomb threat evacuations.

6. Stairway Monitor. Under the direction of the Floor Warden, the Stairway Monitor controls the movement of personnel in the stairway. His duties include:

a. Inspecting complete stairway to insure there are no suspicious items if evacuating for a bomb threat.

b. Immediately establishing a new route of evacuation if a bomb or a suspicious item is located therein.

c. Keeping door open to stairway.

d. Keeping personnel in single file in stairway and instructing them to grasp handrail.

e. Keeping personnel moving steadily at a walking pace and not permitting them to run.

f. Closing door after all personnel in line have passed through door and leaving post when last person passes through door.

7. Elevator Monitor. Under the direction of the Floor Warden, the Elevator Monitor controls the use of passenger elevators. His duties include:

a. Taking position at passenger elevators, assisting the movement of handicapped personnel and Handicapped Persons Monitors into elevator, and restricting elevator use by others.

b. Knowing operation of elevator: how to avoid stopping at certain floors, manual operation, what to do if elevator stops between floors, etc.

c. Maintaining list of handicapped persons on the floor. List and revisions will be given to Floor Warden. List will include the following information about handicapped persons: name, telephone extension, room number, and type of handicap.

d. Capturing all elevators and bringing them to the first floor for use by fire, police or other emergency personnel, after handicapped personnel have been evacuated.

8. Handicapped Persons Monitor. Under the direction of the Floor Warden, the Handicapped Persons Monitor assists physically handicapped persons who would require the use of an elevator to evacuate the building. His duties include:

a. Assisting handicapped persons from their places of work to the elevator, down the elevator, and out of the building.

b. Knowing the location of the handicapped persons who are to be assisted, their types of handicaps, and the location of any wheel chairs, crutches, etc., which may be needed by the handicapped persons.

c. Note elevators are to be used to evacuate handicapped persons only when authorized by the designated official.

9. Ground Floor Exit Monitor. Under the direction of the Ground Floor Warden, the Ground Floor Exit Monitor controls the egress from the building. His duties include:

a. Insuring there are no suspicious items in the route of evacuation if evacuating for a bomb threat.

b. Immediately establishing a new route of egress if a bomb or suspicious item is discovered near the exit of the building, and continued surveillance to ensure personnel are not allowed to come close to the area from either direction.

c. Maintaining his assigned exits clear of obstructions.

d. Opening doors to assigned exits.

e. Preserving order at exit areas inside and outside of building.

f. Keeping people a safe distance from exits and not allowing unauthorized personnel to enter building before the signal to reenter has been given.

10. Messenger. Under the direction of the Floor Warden, the Messenger carries messages. His duties include:

a. Carrying written and verbal messages for the Floor Warden (avoiding walking against traffic where possible).

b. Performing other errands as required by the Floor Warden.

11. Telephone Monitor. Under the direction of the Floor Warden, the Telephone Monitor places telephone calls and relays telephone messages. His duties include:

a. Operating telephone and finding telephone numbers of Organization personnel.

b. Relaying telephone messages to and from the Floor Warden.

12. Medical Officer. The Medical Officer serves as head of the Health and First-Aid Service. He is responsible for training and equipping all personnel assigned to perfrom medical or first-aid services in an emergency, and for supervising emergency first-aid or medical self-help operations within the building during an emergency. His duties include:

a. Arranging with the American Red Cross or other sources for first-aid and medical self-help training for all Organization personnel who need it.

b. Supervising the selection of first-aid or medical treatment areas (in shelters and elsewhere,) as required.

c. Directing first-aid or medical self-help operations and controlling access to medical supplies, as required, to assure their proper use, conservation, and availability for emergency use.

d. Establishing policies and rules governing the emergency treatment of ill and injured persons, the maintenance of adequate sanitation and hygienic standards, and other matters relating to emergency health, hygience, and medical activities within the building during an emergency (or during the occupation of shelter within the building).

(e. Inspecting the storage and handling of food and drinking water in shelter areas within the building.)

13. First-Aid Monitor. Under the direction of the Medical Officer, the First-Aid Monitor administers immediate first-aid to injured personnel. His duties include:

a. Knowing the location of medical supplies and treatment areas.

b. Administering first-aid to injured persons.

c. Knowing the extent of first-aid to be administered and whom to notify if more treatment is needed.

d. In the absence of injured persons on the floor, and when all occupants have evacuated, reporting to the emergency treatment center to assist the Medical Officer.

14. Fire Marshal. The Fire Marshal serves as head of the Fire Service. With the cooperation of the Buildings Manager, he organizes firefighting teams for initial firefighting operations. His duties include:

a. Providing firefighting instruction through available sources.

b. Assuring that firefighters know their stations, locations of fire-fighting equipment in their area of responsibility, and the alarm signals which direct them to their stations.

c. Deploying firefighting personnel to fire areas to extinguish or contain fire pending the arrival of other firefighting forces, and cooperating with such forces upon their arrival.

d. Working closely with the Buildings Manager on matters of fire prevention and protection.

e. During emergencies, he reports to the Control Center.

15. Fire Extinguisher Monitors. Fire Extinguisher Monitors operate hand-type fire extinguishers. Their duties include:

a. Knowing the different types of fires and types of fire extinguishers to use.

b. Being familiar with the operation and capacity of fire extinguishers on their floors.

c. Knowing the location of fire extinguishers and alarm signals which direct them to tneir stations.

d. Using care in operating fire extinguishers to avoid unnecessary damage to personal equipment and records.

e. In the absence of fire in their area, reporting to the Fire Marshal for instructions.

16. Utilities Officer. The Utilities Officer is responsible for controlling building utilities during an emergency. Under tne direction of the Deputy Designated Official, the Utilities Officer serves as head of the utilities control group and performs the following duties:

a. Establishes a plan to attend mechanical devices; ventilation, water, gas, and steam valves; power switches; etc., during an emergency.

b. Dispatches individuals or teams, at the sound of emergency alarms, to prearranged control points for preplanned or directed action.

17. Utilities Control Team. Under the direction of the Utilities Officer, the Utilities Control Team is responsible for controlling utilities during an emergency. During emergencies they report to the Utilities Officer in the basement or other predesignated location.

18. Bomb Search and Reconnaissance Officer. The Bomb Search and Reconnaissance Officer serves as the chief of the Bomb Search Team. He is responsible for recruiting, organizing, training, and equipping, if necessary, all personnel assigned to bomb search activities. He shall establish contact with bomb disposal units of local law enforcement agencies and with the U. S. Army, Explosive Ordnance Disposal Detachments, in his area. Some of the duties and responsibilities of the Bomb Search and Reconnaissance Officer are as follows:

a. Ascertain the structural composition of the building to determine possible explosion effects.

b. Establish a cascade telephone system to alert all team members to effect a building search.

c. Coordinate search activity with local law enforcement search team and/or the U. S. Army Explosive Ordnance Disposal Detachments.

d. Validate the probability of a suspicious item being a bomb before personnel are evacuated (if time permits him to do so.)

19. Bomb Search Team. Members function under the direction of the Bomb Search and Reconnaissance Officer. Members are normally assigned from those positions coming under the responsibility of the Personnel Movement Officer and from available building operations personnel and building guards. Their duties are:

a. Search assigned areas for bombs, suspicious packages, and items that do not fit in with their surroundings.

b. Immediately report any suspicious objects to the Bomb Search and Reconnaissance Officer AFTER all personnel in the immediate vicinity, (next to, above and below the object) have been evacuated.

c. Report to Bomb Search and Reconnaissance Officer when search of assigned area is completed.

*(20. Radiological Officer. The Radiological Officer serves as the head of the Radiological Monitoring Service. He is responsible for organizing, training, and equipping personnel assigned to radiological monitoring functions and for supervising and directing all radiological monitoring activities within the building after a nuclear attack. His duties include, but are not limited to:

a. Training or arranging for the training of all personnel assigned to the Radiological Monitoring Service.

b. Obtaining and providing for the safe storage of radiological monitoring instruments, personnel dosimeters, and related equipment.

c. Insuring that all radiological monitoring instruments assigned to or in the custody of the Organization are maintained in effective operating condition.

d. After occupation of any shelter area in the building, directing and supervising radiological monitoring activities and serving as technical advisor on radiological defense to the Shelter Manager and Coordinator.)

(21. Radiological Monitors. The Radiological Monitors assist the Radiological Officer in the performance of his duties.)

(22. Supply Officer. The Supply Officer is responsible for the care of and issuing to appropriate officials all supplies, especially essential stocks of food, water, medical supplies, sanitation equipment, and radiological monitoring instruments. He serves as head of the Supply Service and performs the following functions associated with shelter management:

a. Plans and schedules distribution of supplies to appropriate leaders, and regulates consumption in conformance with established shelter management policy.

b. Procures, as available, and to the extent storage space permits, desirable items over and above basic stocking through the local government or other possible sources.

c. Establishes a program covering the acceptance and storage of issued supplies and personal supplies; inventories all supplies and equipment; provides for, and maintains, security storage of such materials; and issues daily rations, medicines, and other items to appropriate Organization officials.

d. Trains supply assistants in sufficient numbers to carry out the supply functions of the Plan.)

(23. Supply Assistants. The Supply Assistants assist the Supply Officer in the performance of his duties.)

(24. Welfare Officer. The Welfare Officer is responsible for the rganization and training of a staff of persons who will provide for gistration of shelter occupants and their subsequent needs, such as unit eding, billeting, recreation, information, and religious requirements.)

(25. Welfare Assistants. The Welfare Assistants assist the Welfare Officer in meeting the feeding, billeting, recreation, information, and religious requirements of the shelter occupants.)

*SEE NOTE, PAGE 11.

CHAPTER 4. TRAINING

1. General. A continuing program of training and education for all Organization personnel is imperative to insure maximum effectiveness of the Organization. Personnel who are assigned duties and responsibilities in the Organization will require and shall be given specific training in the skills required to perform their assigned functions, e.g., first-aid, firefighting, elevator operation, etc. The Designated Official is responsible for determining these training requirements for employees assigned to the Organization and for bringing these training requirements to the attention of the appropriate tenant agency officials. (The Designated Official shall also encourage general civil defense education for all Federal employees in the building so that they will be able to cooperate intelligently in self-protection activities and in the community civil defense programs.)

(2. Civil defense training for Federal employees.

a. Executive Order No. 10529 of April 22, 1954 (19 F.R. 2379: 3CFR), provides that heads of Federal agencies may authorize personnel of their respective agencies to participate in civil defense training programs and test exercises in cooperation with any state or political subdivision. Federal employees may be released for periods up to 40 working hours during any calendar year for the purpose of receiving such civil defense training. Agency heads are encouraged to cooperate with their Protection Organizati officials in making personnel available for civil defense trainin under the provision of the Executive Order.

b. Each tenant agency is responsible for assuring that those of its employees who have been assigned duties in the Organization are scheduled for appropriate training in accordance with a training plan to be developed by the Designated Official.)

3. Drills. Organization personnel and building occupants will participate in drills that will familiarize them with the actions they are expected to take in an emergency. Evacuation drills will be conducted periodically under the direction of the Designated Official. Drills should be announced. Occasionally an evacuation drill using alternate means of exit by simulating blocked normal exits will be used.

CHAPTER 5. WARNING AND ALARM SYSTEMS

Civil defense warning signals. The local government is responsible for disseminating civil defense warnings to the public. This usually is achieved through a system of centrally controlled outdoor sirens. There are two civil defense warning signals:

a. ALERT signal. This is a steady tone or blast for three to five minutes which signals the broadcast of essential emergency information. Building occupants will receive further instructions from their Floor Wardens.

b. ATTACK warning signal. This is a wavering tone or series of short blasts for three to five minutes signalling that actual attack against this country has been detected. Upon hearing this warning, personnel should take the best shelter available and keep away from windows. Upon orders from the Floor Warden, they should go to the nearest fallout shelter, if a shelter is not established in the building.

2. Disaster alarm signals. Non-civil defense disasters will be signalled within the building. The signals will consist of a continual striking of bells. The alarm may be given orally.

a. Fire alarm. This is a continual striking of bells signalling a fire in the building. Upon instructions from the Floor Warden, occupants will evacuate the floor or the building. Once the building is evacuated, personnel should clear the immediate area around the building and wait for oral instructions from Organization officials.

b. Other alarms. A continual striking of bells or an oral alarm will be used to warn of natural and other disasters. Natural disasters include earthquakes, floods, and wind storms. Other disasters include explosions, escape of lethal gases, civil disturbances, and bomb threats. Generally, for natural disasters, the Designated Official (after conferring with other officials) will evacuate the building and move personnel to safer areas.

3. Communication requirements. (The Designated Official, in cooperation with others, will assure that arrangements are made with the local civil defense organization for the receipt of civil defense information at the building.) In collaboration with the Buildings Manager, the Designated Official will arrange for communication of warnings within the building. Specific provisions will be made for informing all occupants of the existence of different warning signals, their meanings, and what actions are to be taken. Warning signals will be tested on a regular schedule to insure that the equipment is working properly. Drills should be scheduled often enough to enable the occupants to instantly recognize the sound and meaning of all warnings and to automatically take the proper action.

CHAPTER 6. EMERGENCY AND EVACUATION PROCEDURES

1. Control Center (Room location) (Phone No.) is designated as the location that will be utilized by the Organization in an emergency. All Organization personnel must know the telephone number and location of the Control Center so communications can be established in an emergency.

2. Emergency procedures.

   a. Upon notification by the Designated Official, the Organization will inform the building occupants of the emergency. Emergency actions are shown in appendices A through I.

   b. It is important that the emergency procedures be known in advance of an emergency so immediate action can be taken. Delays caused by looking at instructions after the alarm has sounded could cause injury or death which might be avoided if the occupants were prepared in advance. In addition to the procedures contained in this handbook, which are primarily for Organization personnel, each work station in the building will be provided with emergency procedures.

3. Evacuation procedures.

   a. Under no circumstances should an evacuation take place for a bomb threat, without the evacuation route first being searched for bombs or suspicious items.

   b. Evacuation may be required because of an emergency. Normally, the Designated Official will decide when evacuation orders will be given. He will determine whether one floor, various floors, or all floors will be evacuated. The Floor Warden may decide to evacuate the floor if he thinks there is not sufficient time to consult the Designated Official. In some cases, the Floor Warden will be forewarned of an emergency by the building alarm signals (or civil defense signals outside of the building.) When forewarned, the Floor Warden will instruct floor occupants to line up in the corridor at the stairways.

   c. Each Floor Warden will be told about the emergency, on what floor the emergency exists, the sequence of evacuation, and whether the evacuation will be partial or complete.

      (1) A partial evacuation will involve only the necessary floors and will be accomplished at the direction of the Floor Wardens.

      (2) A complete evacuation of the building involves all floors. If there is not an emergency on a specific floor, evacuation will take place as follows: The ground floor will be evacuated

first, followed by the basement; then in ascending order the second floor, third floor, etc. If there is an emergency on a floor which requires a complete evacuation of the building, the floor on which the emergency exists will evacuate first followed in ascending order by the floors above that on which the emergency exists and then by descending order for floors below the floor on which the emergency exists.

d. Evacuation will utilize the routes shown on the evacuation floor plan which is posted on the bulletin board on each floor. The nature of the emergency may require that the Floor Warden designate an alternate route. If the prescribed routes are blocked or unusable, the Floor Warden may direct the use of fire escapes, but only as a last resort. (See Figure 6-1.)

e. Upon evacuation of the floor or building, each Floor Warden will personally report to the Personnel Movement Officer who will be at the Control Center. Information given by the Floor Warden will help keep Organization officials aware of the progress of the evacuation.

f. Prior to evacuation, building occupants will take the following action whenever possible unless such action would endanger their lives:

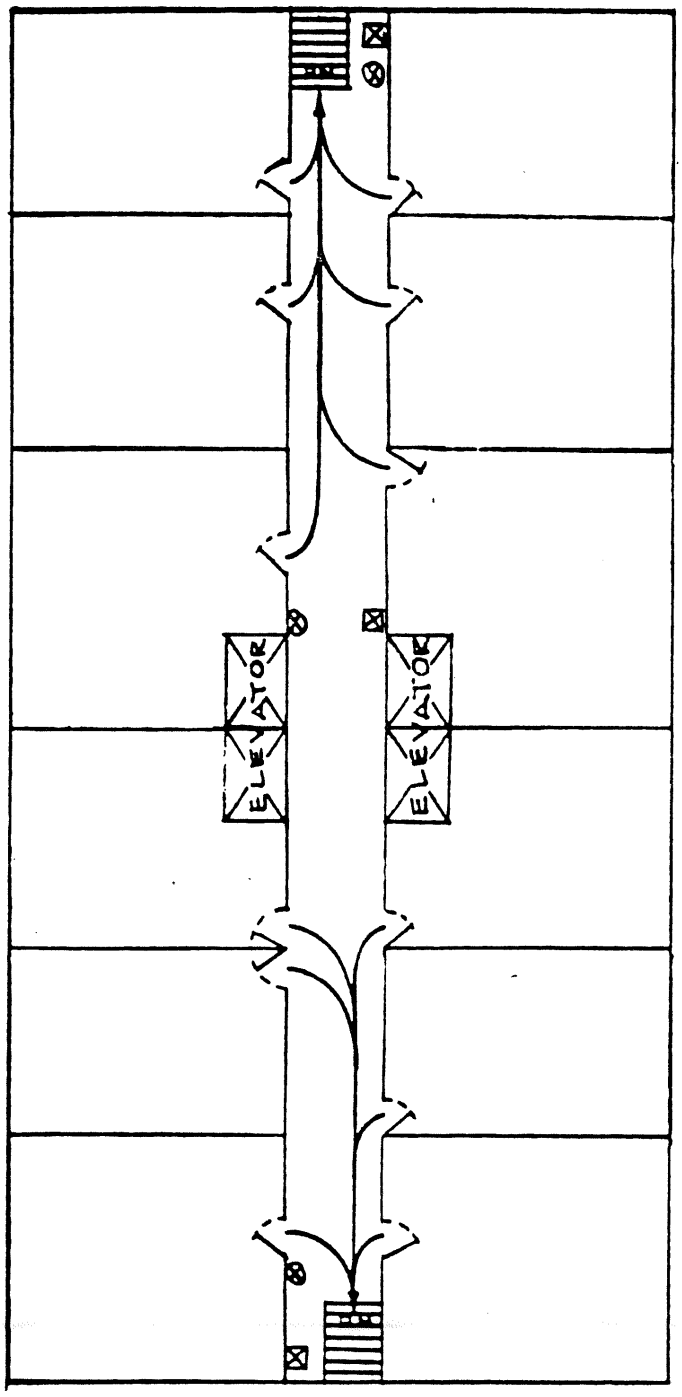
(1) Close windows. (Open for bomb evacuation.)

(2) Place exposed records in cabinets or desk drawers or spread covers over the records to protect them against damage.

(3) Place classified documents in safes and secure their location.

(4) Disconnect electric equipment. (Leave lights on for bomb evacuation.)

(5) Close, but do not lock, the door when the last person leaves the room. (Leave the doors open for bomb evacuations.)



Typical Emergency Evacuation Plan

⊗ Fire Alarm Locations

⊠ Fire Extinguisher Locations

Figure 6-1

FIRE PREVENTION

ggested practices for fire prevention in all buildings:

1. Maintain good housekeeping in all areas of the building; this is one of the most effective means of preventing fire.

2. Bring to the attention of your supervisor any apparent fire safety hazard existing in the building.

3. Obey "No Smoking" signs.

4. Do not throw matches, cigars, cigarettes, or pipe ashes into waste baskets or into any type of receptacle containing combustible material.

5. Oily rags or similar flammable materials in the building must be placed in approved metal containers provided for that purpose.

6. Hotplates, irons, or similar electrical equipment with heating elements may be used in buildings if such appliances are approved by Underwriters' Laboratory and are installed in accordance with local fire codes and Building Manager's approval.

7. Deposit all trash in receptacles provided for that purpose or arrange for its storage in regular trash rooms.

8. Exits and passageways should be kept clear of storage to permit free movement of personnel and firefighting equipment.

FIRE IN BUILDING

1. Upon discovering a fire, occupant notifies the Fire Department by activating nearest alarm box (or calls Fire Department telephone number).

2. Occupant calls or has nearby person telephone or contact Floor Warden and gives him location of fire.

3. Floor Warden telephones Designated Official who will decide whether evacuation will be partial or complete. Floor Warden may decide to evacuate the floor if, in his judgment, there is not sufficient time to call the Designated Official.

4. Fire Extinguisher Monitor uses fire extinguisher to control small fires. In case of a major fire, Floor Warden warns persons in the immediate vicinity to evacuate the affected area.

5. Occupants take the following action when the fire alarm is sounded:

   a. Walk to the corridor and line up near the stairway.

   b. Obey the instructions of the Floor Warden and the monitors.

   c. Proceed into the stairway in an orderly manner as directed by the Stairway Monitor and grasp the handrail while walking up or down stairs.

   d. Walk to the area specified by the Floor Warden and stay in formation.

   e. If there is a complete evacuation, move at least 300 feet away from the exits and wait for instructions from Organization officials.

   f. If time permits, close windows, put classified documents in safe or secure location, place exposed records in cabinets or desk drawers or spread covers over records to protect them, and disconnect electric equipment. The last person to leave the room closes but does not lock the door.

6. Designated Official and Buildings Manager will have copies of specific plans and instructions for each area of the building. Plans are to be on file and kept current.

Appendix 6-B

Guides. The following additional guides are established to assist in preparing for and minimizing the effects of emergencies. Necessarily, the guides are general in nature and are provided for adaptation and application as required by local circumstances.

a. Protection of priority locations. Locations requiring priority protection (switchboards, teletype centers, heating plants, induction centers, etc.) should be identified in advance and arrangements made for protection of these locations. Consideration should be given to the use of existing heavy monumental-type metal doors, gates, etc., when available, as physical barriers to deter penetration of selected priority locations. Also, use of readily available materials such as plywood could be helpful in boarding up windows and other vulnerable openings. Types of actions considered essential are:

(1) Planning and inspecting. Survey the premises of particular occupants whose locations have or may be reasonably expected to be the subject of civil disorders or demonstrations to determine whether some of the entrances to the building should be closed; whether door latches are adequate and tamper resistant; whether the space lends itself to installation of practical types of intrusion and fire alarm systems; and whether it would be feasible to use fire-resistant file cabinets or to install automatic fire extinguishing systems to minimize fire losses and deter vandalism.

(2) Suspicious actions. All personnel, particularly guards, crafts, and custodial personnel, shall be alerted to observe and report immediately any threats and suspicious looking persons, packages, or equipment in any building.

(3) Building service spaces. All doors to building service areas, such as mechanical rooms, transformer vaults, slop sink rooms, wire closets, etc., should be locked at all times when possible with access allowed only to authorized personnel. Consideration should be given to removing identification signs on doors to these building service areas.

(4) Communications areas. Guidelines for protective measures to be taken for these areas have been issued by the Commissioner, TCS, in a memorandum dated September 30, 1969.

(5) Stairwells and restrooms. Particular attention should be given to closets not capable of being locked, restrooms, stairwells, and other areas where explosives might be secreted.

(5) Key control. Key control should be in strict conformance with the Building Manager's regulations.

(7) After-hour entry. Identifying and recording the presence of all persons entering or leaving the building after normal duty hours is essential.

2. In case of a bomb threat, perform the following actions:

a. Upon learning of a bomb threat:

(1) Person receiving call about a bomb threat should attempt to get exact location within building where bomb has been or is going to be planted. Attempt to get as much information as possible about the caller, e.g., vocal idiosyncrasies, race, sex, group affiliation, etc. Listen for noises in background or for other clues which might indicate caller's identification and location. Information received should be carefully recorded and given to the Control Center or the Designated Official. The Designated Official in turn will notify the local police, FBI and the U. S. Attorney.

(2) Person receiving letter or card announcing a bomb threat will give it to the Control Center or Designated Official.

b. The recipient telephones the Control Center or Designated Official and explains situation.

c. Designated Official notifies Bomb Search and Reconnaissance Officer and initiates search procedure and establishes end of search time. Personnel assigned to bomb search activities must be properly trained. Bomb Search and Reconnaissance Officer initiates telephone cascade system to alert all team members to effect a building search. All searches are visual. A suspicious item is never moved or disturbed.

(1) Floor Warden organizes search on the floor.

2) Zone Monitors search their assigned areas.

3) Stairway and Elevator Monitors search their assigned areas, restrooms, and utility rooms off the corridors.

(4) Available guards, building maintenance men, and custodial personnel report to the Control Center for assignment. At their assigned floor, they work under the direction of the Floor Warden.

(5) Searchers work in pairs and move with extreme caution, both during the search and after the bomb is located.

(6) Upon completion of a thorough search of their areas, searchers report to the Floor Warden.

(7) At a predetermined time each Floor Warden telephones the emergency operation center and reports the progress of the search on his floor.

d. In the event a suspicious-looking object is found, finder performs the following actions:

(1) He does not remove or disturb the suspect object.

(2) He immediately evacuates all persons from the vicinity.

(3) He notifies the Bomb Search and Reconnaissance Officer that a suspect object is found and informs him of its location.

(4) If time permits, the Bomb Search Officer verifies if the object is suspect.

e. Designated Official orders an immediate evacuation of floors near the affected area and notifies local police and/or the the nearest military Explosive Ordnance Detachment (EOD).

f. Guard is stationed at building entrance and directs police and/or EOD bomb disposal team to location of bomb.

g. After disposal of the bomb, Designated Official gives signal for occupants to return to their offices.

DEMONSTRATIONS

1. No single standard procedure can be established for all demonstrations as they will vary in their nature and the problems they present because of the character and number of the participants and the atmosphere in which demonstrations occur. Thus, any suggestions in any plan must have sufficient flexibility to fit the situation as it develops.

2. To develop appropriate plans in handling demonstrations, it is necessary to first determine the type of criminal jurisdiction designated for the property. The types of criminal jurisdiction are as follows. (Note: the jurisdiction appropriate to each building should be included in each FSPO.)

Exclusive jurisdiction -- the United States has sole authority over the site; arrests made at the site by a state or local officer for violation of a state statute would be invalid, and the state or local courts would be without authority to try persons so arrested.

Concurrent jurisdiction -- the United States and the State jointly exercise the authority to enforce laws on the site. The specific circumstances of each case determine which entity enforces the law.

Partial jurisdiction -- usually concerns legislated matters in which the United States and the State in which the site is located exercise overlapping authority. The State reserves authority in non-criminal matters (e.g., taxing private property).

Proprietorial interest -- the United States has not obtained any measure of the State's authority over the site, but it still possesses rights of ownership and certain powers and immunities not held by private landholders. In this instance, the State has sole criminal jurisdiction.

3. The handling of demonstrations, "sit-ins", etc., has been the subject of discussion among officials of the Department of Justice and it has been determined that the Designated Official will handle such matters in close cooperation with the office of the United States Attorney in the area concerned. There must be mutual understanding of the action to be taken in such matters and assurance that such action is undertaken with legal authority and will not violate civil rights. The Designated Official is the point of liaison for all building tenants in the planning and execution of action for handling demonstrations. (SEE CHAPTER 1, PARAGRAPH 4.a., FOR DESIGNATED OFFICIAL RESPONSIBILITIES CONCERNING DEMONSTRATIONS.)

4. The following pertinent facts should be learned prior to demonstrations so that appropriate plans may be prepared:

a. Applicable type of criminal jurisdiction.

b. Name of sponsoring organization.

c. Time of demonstration.

d. Proposed schedule of events.

e. Exact location.

f. Activities planned.

g. Purpose of demonstration.

h. Projected attendance.

i. Character and temperament of those expected to participate.

5. The Designated Official should meet with tenant agencies, local police, United States Attorney, and United States Marshal, as appropriate.

a. The cascade plan of communication, as contained in other sections of the FSPO, should be reviewed to ensure continuity of information and necessary action between the building tenants.

b. When a demonstration is expected to take place on GSA-controlled property, guards and other personnel shall be instructed in accordance with the plan of action agreed upon with the U. S. Attorney. Instructions will vary. They may include permitting the demonstration to take place provided that entrances are kept clear and Government property and operations are not adversely affected; participating in arrangements for a meeting of a representative group of demonstrators with appropriate Government officials; prohibiting entry into the facility by persons who parade bearing signs or who by other actions identify themselves as participants; calling on enforcement resources for assistance; etc. It is desirable to use procedures which appear most likely to gain the cooperation of the demonstrators.

c. Agreement should be reached regarding the circumstances under which arrests may be necessary and the course of action to be followed in effecting such arrests. (In many instances arrests are openly sought by demonstrators. Arrests should be made only when necessary.)

6. Plans should be made as to action to be taken if persons gain entrance to the building and then begin a demonstration, either individually or as a group. Normally, demonstrators shall be asked to leave; if they refuse, become disorderly, or offer passive resistance, i.e., lie or sit on the

floor, it may become necessary to place them under arrest. An alternati to arrest is removing demonstrators from the building and restricting re-entry. Again, arrests should be avoided so far as possible. Necessa arrests should be carried out under the guidance of the U. S. Attorney.

Appendix 6-D

EXPLOSION

In the event of an explosion in the building, such as those caused by leaking gas or a faulty boiler, perform the following actions:

1. Occupants take cover under tables, desks, or other such objects which will give protection against flying glass or debris.

2. Occupant notifies the Fire Department by activating nearest building alarm box.

3. Occupant calls, or has nearby person contact, Floor Warden to give him location of explosion.

4. Floor Warden telephones the Designated Official and explains the situation.

5. After effects of explosion have subsided, Designated Official will decide whether to evacuate the building.

6. If an evacuation is necessary, occupants evacuate under the direction of the Floor Warden.

7. If the building is evacuated, occupants wait outside the building for instructions from Organization officials.

CHEMICAL ACCIDENT

Chemical accidents of disaster magnitude would include tank truck accidents involving large quantities of toxic gases. Should such an accident endanger the occupants of the building, perform the following actions:

1. Occupant notifies Floor Warden of danger.

2. Floor Warden telephones Designated Official and explains the situation.

3. Designated Official decides whether to evacuate the building.

4. If an evacuation is necessary, occupants evacuate under direction of the Floor Warden.

5. Designated Official telephones the Fire Department and explains the situation.

6. First-Aid Monitors administer first-aid.

7. Occupants avoid fumes by moving crosswind; they should never move upwind or downwind.

SEVERE WINDSTORM

e U. S. Weather Bureau can forecast severe windstorms with a high degree accuracy. However, if high winds develop during working hours with little or no warning, perform the following actions:

1. Designated Official will decide whether to evacuate to a designated shelter on each floor or to a shelter in the basement.

2. Occupants will evacuate under direction of the Floor Warden; they should remain near inside wall (on the lower floors if possible), avoid rooms with large roof spans, and close windows and blinds.

3. Utilities Control Officer notifies the Buildings Manager and the Designated Official of any damage to the building or utilities.

4. Designated Official keeps a radio tuned to a local station for the latest weather information.

EARTHQUAKE

The _____(Name of Area)_____ is subject to earthquakes. There will be n advance warning.

1. Upon feeling a serious quake, occupants perform the following actions:

   a. Obtain shelter under tables, desks, or other such objects which will offer protection against flying glass or debris. If possible, keep at least 15 feet away from windows to avoid flying glass. Step under a doorway or into a narrow hall or corridor. Keep away from skylights and large overhead light fixtures.

   b. Do not leave cover until advised to do so.

   c. If evacuation is necessary, evacuate under the direction of the Floor Warden.

   d. Do not run outdoors. Upon leaving building, watch for falling debris or electric wires.

   e. Proceed to a safe area, away from the danger of being struck by falling debris or electric wires.

   f. Take precautions against additional shocks.

2. Designated Official will notify the Fire Department of any fires.

3. Some of the following conditions may exist in conjunction with or following a serious earthquake:

   a. Presence of dead, injured and sick. Some may be trapped in buildings or debris.

   b. Disorder and unrest, including looting and panic.

   c. Fire.

   d. Shortage or contamination of drinking water.

   e. Shortage of water for firefighting.

   f. Shortage of food supplies.

   g. Extensive damage to buildings and structures making them potential dangers to life and safety.

h. Disruption of gas and electric power systems.

i. Disruption of some or all communications facilities.

j. Shortage of living accommodations due to the destruction of buildings or influx of refugees.

k. Blocked streets, hignways, roads, bridges, etc., which are not safe for travel.

l. Major or complete disruption of public and private transportation facilities.

m. Danger of widespread epidemic, due to water contamination and breakdown of public health control.

n. Shortage of medical supplies and hospital facilities.

o. Disruption of regular governmental operations.

p. A large-scale evacuation of populace from the metropolitan area.

4. Immediately after an earthquake, Organization personnel perform the following actions:

a. Administer first-aid, assist in rescue operations - as dictated by necessity. (Move seriously injured to emergency treatment center.)

b. Turn off utilities: gas, electricity, and water.

c. Inspect all utility lines for damage.

d. Extinguish fires. (Do not light fires after an earthquake.)

e. Reserve telephones for emergency calls only.

f. Look for other hazards such as broken glass, spilled fluids, damaged equipment, loose plaster, crumbling ceilings, etc.; if found, take corrective action.

g. If required, request assistance from outside sources (Disaster Corps).

h. Turn on radio for information about the extent of community damage.

i. Make every effort to carry out routine procedures and return building to normal operation.

ENEMY ATTACK

Civil defense signals warning of an enemy attack are sounded by sirens operated by the City and County of (Name of city and county).

1. ALERT signal. This is a steady blast or tone for three to five minutes signifying that essential emergency information will be broadcast.

   a. If evacuation is necessary, occupants evacuate according to directions of the Floor Warden.

   b. Occupants take personal possessions (coats, purses, food) when leaving work station.

2. ATTACK WARNING signal. This is a wavering tone or a series of short blasts for three to five minutes; it signifies that actual attack against this country has been detected.

   a. Occupants perform the following actions:

      (1) Take cover under desks, tables or any large objects which will give protection against flying glass or debris.

      (2) Stay against the wall nearest the windows for protection.

      (3) Leave cover only when directed to do so by the Floor Warden.

      (4) When so directed, proceed to fallout shelter. The fallout shelter is shown on the evacuation floor plan which is posted on the bulletin board on each floor. If there is no designated shelter area in the building, proceed to the nearest building with an approved shelter area.

      (5) Remain in shelter until other action is directed by Shelter Official.

   b. Designated Official will contact appropriate authorities for further action to be taken concerning his building.

PANIC

1. Panic defined. Panic may occur during an emergency. The ability to control panic may save lives and reduce injuries. Panic is defined as "A sudden, unreasoning, hysterical fear, often spreading quickly." Panic is caused by fear, although those involved may not know what they fear. People may be tempted to join a fleeing crowd; the fright of those in motion is enough to suggest the presence of something to fear. When this happens it may be difficult to control the crowd. Attempting to reason with them may be futile, but it may be possible to control them by assuming leadership or by reassuring key members of the group.

2. Panic deterrents. The likelihood of panic, and the physical causes of panic can be eliminated by an effective program of informing tenant agency personnel of what is expected of them in an emergency. In an emergency, the Organization should be prepared to remove the injured and the dead from general view, clear away debris which appears to cut off escape, quickly control fire, and approach any disturbance with calmness. Emergency preparations should include arrangements to delineate clear routes to be taken in evacuating the building or going to shelter; they should also designate the placing of Organization personnel where they can take command of an emergency and give calm, decisive instructions at places where groups are likely to congregate.

3. Antidotes for panic. In certain circumstances, it is conceivable that, despite emergency preparations, an unorganized group may be on the verge of panic. Organization personnel should be prepared to deal with this situation according to the following principles:

a. Provide assurance. Reassure the group by giving information and instructions calmly.

b. Eliminate unrest. Dispel rumors. Identify troublemakers and prevent them from spreading discontent and fear.

c. Exert positive leadership. Decisively propose positive actions. Assert what to do, rather than what not to do.

INSTRUCTION SHEET FOR
INITIAL BOMB THREAT REPORT

CHECK WHETHER REPORT IS AN ORIGINAL OR CHANGE TO AN ORIGINAL.

1. PRINT THE EXACT WORDS USED BY THE THREATENER.

2. TIME THREAT WAS RECEIVED. SHOW IF A.M. OR P.M.

3. DATE OF THREAT.

4. DID THREATENER SAY WHEN IT WOULD GO OFF? IF SO, STATE TIME.

5. DID THREATENER STATE A LOCATION WHERE THE DEVICE IS SUPPOSED TO BE PLANTED?

6. ITEMS A THROUGH D. LIST NAME, ADDRESS AND TELEPHONE NUMBER IF GIVEN BY THE THREATENER OR IF KNOWN, AND WHETHER THE PERSON WAS MALE OR FEMALE.

   ITEM E. STATE IF THREAT MODE WAS BY PHONE, LETTER, OVERHEARD CONVERSATION, ETC.

   ITEM F. STATE IF PERSON SOUNDED HIGHLY EDUCATED, USED POOR GRAMMAR, ETC.

   ITEM G. STATE IF THE PERSON HAD ANY TYPE OF FOREIGN ACCENT.

   ITEM H. WAS THE PERSON'S LANGUAGE PECULIAR TO A REGION, COMMUNITY, SOCIAL GROUP, OR OCCUPATIONAL GROUP?

   ITEM I. CHECK THE AGE GROUP THAT COMES CLOSEST TO THE SOUND OF THE VOICE.

7. CHECK YES OR NO BLOCK. AN EXAMPLE OF FAMILIARITY WOULD BE IF THE CALLER SAID, "THERE IS A BOMB ON THE FIRST FLOOR AND I WORK ON THAT FLOOR".

8. DID THE THREATENER STATE ANY PARTY AFFILIATION SUCH AS, STUDENTS FOR A DEMOCRATIC SOCIETY, UNDERGROUND WEATHERMEN, AMERICAN NAZI PARTY, ETC?

9. WAS ANY REASON GIVEN, SUCH AS A RECENT GOVERNMENT DECISION, OR WAS THE PERSON RECENTLY LAID OFF OR FIRED?

10. WAS A CERTAIN TYPE OF DEVICE IDENTIFIED SUCH AS A BOMB, INCENDIARY DEVICE, PIPE BOMB, ETC.

11. DID THE THREATENER SOUND ANGRY, MATTER-OF-FACT, AFRAID OR AS THOUGH HE WAS JOKING?

12. COULD ANYTHING BE HEARD IN THE BACKGROUND, SUCH AS STREET OR OFFICE NOISES, MUSIC, YOUNGSTERS LAUGHING, ETC?

13. LIST LOCAL WEATHER CONDITIONS SUCH AS SUNNY, SPRING-LIKE, RAINING, ETC.

14. HAVE THERE BEEN ANY RECENT RIOTS, DEMONSTRATIONS, BOMBINGS, ETC., IN THE AREA?

15. CIRCLE DAY OF WEEK. CHECK WHETHER OR NOT A PAYDAY, AND IF A DAY BEFORE A HOLIDAY, A HOLIDAY WEEKEND, ETC.

16. INCLUDE ANY INFORMATION NOT COVERED ABOVE SUCH AS IF THE THREATENER HUNG-UP RAPIDLY, BREATHED HEAVILY, STAYED ON THE LINE SILENTLY BEFORE HANGING-UP, TRIED TO DISGUISE HIS VOICE, ETC.

17. PERSON WHO RECEIVED THE THREAT.

18. PERSON WHO REPORTED THE THREAT. IF NOTIFIER (18) IS NOT THREAT RECIPIENT (17), STATE IN 16, RELATIONSHIP TO THREAT RECIPIENT SUCH AS RECIPIENT'S SUPERVISOR, CO-WORKER, ETC.

19. PERSON WHO COMPLETED THIS FORM.

INITIAL BOMB THREAT REPORT

__ ORIGINAL

__ CHANGE TO AN ORIGINAL

1. EXACT WORDS USED IN BOMB THREAT: _____ _____

_____

_____

2. TIME: _____ 3. DATE: _____ 4. DETONATION TIME: _____ 5. STATED LOCATION: _____

6. THREATENER'S

A. NAME: _____ B. __ MALE __ FEMALE

C. ADDRESS: _____

D. TEL. NO: _____ E. THREAT MODE: _____

F. LANGUAGE: _____ G. ACCENT: _____ H. DIALECT: _____

I. AGE: __ UNKNOWN __ CHILD __ TEENAGER __ YOUNG ADULT

__ ADULT __ ELDERLY

7. DID THREATENER INDICATE A FAMILIARITY WITH THE BUILDING? __ YES __ N

IF YES, HOW?

_____

8. ASSOCIATION: _____

9. REASON: _____

10. TYPE OF DEVICE: _____

11. MANNER OR TONE OF THREATENER: _____

12. BACKGROUND NOISE: _____ 13. WEATHER: _____

14. LOCAL AREA ACTIVITY: _____

15. DAY OF WEEK: S M T W T F S PAYDAY: __ YES __ NO HOLIDAY-WHEN: _____

16. MISCELLANEOUS: _____

_____

Appendix 6K-2

17. THREAT RECIPIENT: _____

NAME TEL. NO. ROOM NO. DATE/TIME

_____

POSITION TITLE AGENCY ADDRESS

18. NOTIFIER: _____

NAME TEL. NO. ROOM NO. DATE/TIME

_____

POSITION TITLE AGENCY ADDRESS

19. RECORDER: _____

NAME TEL. NO. ROOM NO. DATE/TIME

_____

POSITION TITLE AGENCY ADDRESS

___ FPSD ENFORCEMENT BRANCH-

___ DIRECTOR, FED. PROT. SERV. DIV.-

___ REGIONAL COMMISSIONER, PBS-

___ REGIONAL ADMINISTRATOR -

___ FPSD TECH. SERVICES BRANCH

___ SPECIAL EVENTS CADRE-

___ FED. PROT. SERV. DIV. ZONE NO.____

___ REGIONAL DIR., BUSINESS AFFAIRS-

___ OTHER:

DISTRIBUTION

Appendix 6K-2

INSTRUCTION SHEET FOR FOLLOW-UP REPORT

PLACE THE TIME AND DATE OF THE INITIAL REPORT IN THE UPPER RIGHT CORNER. THE TIME AND DATE IS ON THE INITIAL REPORT AT NUMBERS 2 AND 3. IF AN INITIAL REPORT HAS NOT BEEN COMPLETED AND A SUSPICIOUS PACKAGE OR BOMB IS FOUND, OR IF A BOMB FUNCTIONS, INCLUDE THE AGENCY NAME, BUILDING NAME, LOCATION, AND ADDRESS IN MISCELLANEOUS (9).

1. INCLUDE ALL AGENCIES NOTIFIED SUCH AS THE ARMY, POLICE AND FIRE DEPARTMENTS, ETC. DO NOT INCLUDE THE OFFICES LISTED ON THE BOTTOM OF THE FORMS.

2. SELF-EXPLANATORY.

3. SELF-EXPLANATORY.

4. SELF-EXPLANATORY. IF EXACT NUMBER OF PERSONS IS NOT KNOWN, ESTIMATE NUMBER.

5. SELF-EXPLANATORY.

6. DESCRIBE ITEMS FOUND, WHO WAS NOTIFIED, AND ACTION THAT WAS TAKEN TO REMOVE AND IDENTIFY THE ITEMS, ENSURE AT THE TIME ACTION IS TAKEN, THAT A FINAL REPORT WILL BE SUBMITTED, SO IT WILL BE KNOWN WHAT THE ITEMS WERE, WHAT WAS DONE TO THEM, AND WHERE THEY CAN BE LOCATED.

7. SAME AS 6.

8. SELF-EXPLANATORY. DESCRIBE PHYSICAL DAMAGE IN AS MUCH DETAIL AS POSSIBLE.

9. SEE FIRST PARAGRAPH ABOVE. ALSO INCLUDE ANY INFORMATION NOT COVERED ELSEWHERE ON THE FORM.

10. OTHER ACTIONS TAKEN TO INCREASE SECURITY IN THE BUILDING.

11. PERSON COMPLETING THE REPORT.

FOLLOW-UP ACTION ON BOMB THREAT REPORT

INITIAL REPORT TIME AND DATE:
(ITEMS 2 & 3)

1. AGENCIES NOTIFIED OF INITIAL REPORT:

_____

2. PUBLIC AREA SEARCH CONDUCTED: ___ YES ___ NO

3. COMPLETE SEARCH OF ALL ROOMS/OFFICES CONDUCTED: ___ YES ___ NO

4. EVACUATION: PARTIAL ___ YES ___ NO COMPLETE ___ YES ___ NO

NO. OF PERSONS: _____ TIME EVACUATION BEGAN: _____

TIME EMPLOYEES RETURNED: _____

5. INCREASED SECURITY: WAS PACKAGE INSPECTION/IDENTIFICATION INSTITUTED:

___ YES ___ NO

WERE ENTRANCES AND EXITS PLACED UNDER CONTROL: ___ YES ___ NO

WAS PERSONAL IDENTIFICATION REQUIRED TO ENTER THE BUILDING: ___ YES ___ NO

6. WERE SUSPICIOUS ITEMS FOUND: ___ YES ___ NO

DESCRIPTION OF ITEMS: _____

ACTION TAKEN: _____

FINAL IDENTIFICATION & DISPOSITION OF ITEMS: _____

_____

7. BOMB DEVICE FOUND: ___ YES ___ NO

DESCRIPTION OF ITEMS: _____

ACTION TAKEN: _____

FINAL IDENTIFICATION & DISPOSITION OF ITEMS: _____

_____

Appendix 6K-4

8. BOMB DEVICE FUNCTIONED: ___ YES ___ NO TIME: _____

DATE: _____ LOCATION: _____ FLOOR: _____

NUMBER OF PERSONS KILLED: _____ NUMBER INJURED: _____

DOLLAR ESTIMATE OF DAMAGE: _____ AMOUNT OF PHYSICAL DAMAGE: _____

_____

9. MISCELLANEOUS: _____

_____

10. OTHER ACTIONS TAKEN: _____

_____

11. RECORDER: _____

NAME TEL.NO. ROOM NO. DATE/TIME

_____

POSITION TITLE AGENCY ADDRESS

___ FPSD, ENFORCEMENT

___ DIRECTOR, FED. PROT. SERV. DIV.-

___ REGIONAL COMMISSIONER, PBS-

___ REGIONAL ADMINISTRATOR-

___ FPSD, TECH. SVCS BRANCH

___ SPECIAL EVENTS CADRE-

___ FED. PROT. SERV. DIV. ZONE NO. _____

___ REGIONAL DIR., BUSINESS AFFAIRS-

___ OTHER:

DISTRIBUTION

PREVENTION OF THEFTS IN THE BUILDING

The prevention of thefts of both Government and personal property in this building is everyone's concern. Personnel should be aware of the types of thefts that may occur and take precautionary measures to minimize losses.

Thefts of calculators, electric typewriters, and adding machines are sometimes attempted by concealing the items in cardboard containers until they can be taken from the building, often in the guise of being trash. Containers used for this purpose may be similar to the type normally used in custodial or crafts operations. Actual removal is likely to occur just before building security hours go into effect, but it could take place later. Unattended containers in hallways and work areas at any time of the day should be investigated. No carton or container should be taken for granted regardless of how routine its presence or how innocuous its appearance may seem.

Extreme caution should be taken with personal items such as purses, pocketbooks, loose change, etc. Most of these thefts occur during working hours and are often a result of employees carelessly exposing such items on desk tops. Reductions in these occurences can be made if personnel exercise more care in handling their personal property.

Most personal thefts involve purses being removed from desk tops. (Place them in the rear of a file drawer, and lock it if the office is not manned at all times.) Do not keep loose change such as coffee funds or stamps in desks. There have been a number of cases where money was removed from an unlocked desk. Subsequently the desk was locked and broken into because the thief knew money was kept in the desk previously. Money has been removed from locked file cabinets because the key to the cabinet was kept in the desk drawer. If valuables have been kept in an office or desk for years, it is no indication that they will not be missing tomorrow. Also, leaving an office unattended for only two minutes does not increase security more than leaving it for two hours. If it takes a thief ten to fifteen seconds to steal an item, he doesn't care if a person is going to be gone two minutes or two hours. The thief is only interested if a person is going to be gone fifteen seconds. USE COMMON SENSE:

THE GOVERNMENT DOES NOT REIMBURSE INDIVIDUALS FOR THE LOSS (THEFTS) OF PERSONAL ITEMS.

DO NOT LEAVE ANY PERSONAL BELONGINGS UNATTENDED IN THE OFFICE THAT YOU ARE NOT WILLING TO LOSE.

Valuables, such as purses or pocketbooks, should be kept in locked containers, such as a file cabinet, during working hours. A personal item that has monetary or sentimental value is NOT secure when left in an office at night - regardless of the precautions taken. If the loss of a personal item justifies the submission of a theft report, the item was not adequately secured during the day, or should not have been left in the office overnight.

Suspicious or unusual situations or loss of property should be reported to the (Guard Office) (Building Manager) on extension:_____

Appendix 6-L

Facility Protection Checklist

1. Has a Facility Self-protection Designated Official been designated?
2. Has an advisory committee of appropriate tenant officers been set up to assist in the development of the facility protection plan?
3. Has a written self-protection plan been prepared for the facility?
4. Has a self-help organization been formed for the protection of life and property in and around the facility? (Date it was last revised).
5. Have arrangements been made for receiving and disseminating warnings?
6. Have a control center and a communications system been established for use in emergency?
7. Have emergency shut-down procedures been developed?
8. Does the plan provide for enlarging existing protective groups (e.g., guard forces, firemen, etc.) for use in an emergency?
9. Are employees informed about the facility self-protection plan?
10. Are drills or exercises held to test the plan?
11. Have arrangements been made for emergency repair and restoration?
12. Have tenant agencies included self-protection information in their employee publications?
13. Is there an emergency sticker on each phone showing who to call in case of a bomb threat, suspicious package or other emergency?
14. Is there a central location where all emergency calls are received?
15. Have central location personnel been checked to insure they know who to notify for each type of emergency?
16. Are office exits and corridor intersections posted with warning/emergency signals and evacuation routes?
17. Has it been over a year since the last practice evacuation?
18. Are organization personnel readily identifiable through the use of arm bands or hard hats?
19. Have wardens and monitors been equipped with flashlights?
20. Do bomb reconnaissance personnel have extendable angled mirrors for looking under and behind furniture?

21. Has the Director, Federal Protective Service Division, Region 3 (3PS), been requested to conduct a non-evacuation audit (test) of the facility self-protection organization?

*(22. Have sufficient building occupants been trained in civil defense skills (shelter management, radiological monitoring, first-aid and medical self-help, decontamination, firefighting, utilities control, bomb reconnaissance, etc.)?)

(23. Have preparations been made for assessing and reporting damage after attack?

(24. Has liaison been established with the local Civil Defense director?)

(25. Has the facility plan been coordinated with the civil defense plans of the jurisdiction in which the facility is located?)

(26. Have the coordinator and the chief officers of the self-protection organization been trained in civil defense schools?)

(27. Has fallout shelter been provided for building occupants and the public?)

(28. Have plans been made for the movement of building occupants to fallout shelter within the building or elsewhere?)

(29. Has the facility fallout shelter been marked and stocked?)

(30. Has information about personal and family survival been distributed to all building occupants?)

*SEE NOTE, PAGE 11

* U.S. GOVERMENT PRINTING OFFICE : 1978 O-273-866/6440